研究室

日本監査役協会「監査役に期待されるITガバナンスの実践」の解説

トーマツ企業リスク研究所 主席研究員 **楠 正彦**

平成23年8月に公益社団法人日本監査役協会（以下「日本監査役協会」という）のITガバナンス研究会より、「監査役に期待されるIT ガバナンスの実践」という報告書（以下「本報告書」という）が公表された。本報告書は企業におけるITの利活用の進展に伴いリスクが高まっていることを踏まえ、監査役の立場からITガバナンスをどのように理解し、取り組めば良いかについて、フレームワークと最低限留意すべきポイントを提示している。

本稿では本報告書の前半に記載されたITガバナンスの総論部分、すなわちITガバナンスへの取組みのフレームワークについて概要を紹介するとともに、ITガバナンスの確立に向けて、監査役の方々のみならず取締役あるいは管理者の方々がどのような点に留意して取り組むべきかについて解説したい。

なお、本文中の意見に関する部分は筆者の私見である旨、予めお断りしておく。

1．本報告書の構成と本稿の目的

日本監査役協会では平成13年に「ITガバナンスにおける監査役の役割」という報告書を公表しているが、企業におけるその後の経営環境の変化とITの利活用の進展、およびそれらに伴うリスクの増大を踏まえて、ITに精通していない監査役であっても実務においてすぐに活用できる内容に改めたものとして、本報告書が作成、公表された。

本報告書は、

第Ⅰ部　IT環境における監査役の役割と責任

第Ⅱ部　監査役としてのITガバナンスの取組み方

の2部から構成されており、第Ⅰ部ではITガバナンスへの取組みの全体像を示しており、第Ⅱ部ではITガバナンスの実現に向けて最小限何をすべきかについて会社法施行規則に基づいた取組みのポイントを中心に示している。なお、本報告書は具体的なQ&Aも交えてITに詳しくない方にも分かりやすく記載されているので、監査役の方に限らず、取締役あるいは業務管理に携わる方々も含め、ITリスクに関わりのある多くの人が読まれることを推奨する。

以下、本稿では本報告書の第Ⅰ部の概要をその構成に沿って紹介し、解説を加えていく。読者のITガバナンスへの取組みの一助となれば幸いである。

2. ITガバナンス概念登場の背景

本報告書ではITガバナンス概念が登場した背景について、「従来の「IT管理」という管理者層による部門別管理（とりわけ情報システム部門だけに依存した管理）では、全社的なITの利活用をめぐるさまざまなリスクに十分に対応できなくなり、取締役のリーダーシップのもと、全社的あるいは企業グループとしての取組み体制を確立するために登場した概念が「ITガバナンス」である」[*1]と述べている。

また、情報システムは「その影響の大きさゆえに、情報システムの戦略性と、安全かつ効率的な運用は、株主等のステークホルダーにとっても大きな関心事となってきている」[*1]ことから、「監査役も、取締役の責務としての情報システムの運用体制の監視・検証を通じて、ITガバナンスの一翼を担うことが強く求められるようになってきている」[*1]として、監査役がITガバナンスに取組む意義を示している。

解説

歴史的にはITが企業活動において広く利活用されるようになるにつれて情報システムを安定的に稼動させることが重要となり、システムの信頼性や可用性、保守性などを維持、向上させるための各種手法が開発され、IT管理として体系化されてきたという経緯がある。このため、従来のIT管理はどちらかというとプログラムバグの除去であるとか、障害復旧時間の短縮、不正アクセスによる改ざん防止といったテクノロジー視点でのリスク対応が主であったと考えられる。

一方、企業内のみならず対外的接続においてもITが広範に利活用されている現在においては、システム運用ミスによるシステム停止がサプライチェーンやサービスを受ける顧客などに多大な影響をもたらしたり、アクセスコントロールの不備により個人情報漏えいが発生してその対応に時間と費用がかかるだけでなく、企業の信頼を喪失してしまうといった話が珍しくなくなってきている。このようなリスクはその影響度から見て経営層が対応すべき経営リスクであり、経営リスクの視点でITリスクへの取組み体制を確立することがITガバナンスである。

3. コーポレート・ガバナンス、ITガバナンス、IT管理の関係

本報告書は、「ITガバナンスは、コーポレート・ガバナンスの一側面であって、取締役の職務執行の一部としてのITの利活用に関する全社的あるいは企業グループとしての推進体制と、監査役による独立的監視・検証を通じた取締役への規律付けからなる」[*1]と述べている。

また、「ITガバナンスは、コーポレート・ガバナンスのうち、「ITの利活用に伴う企業価値の毀損」（ダウンサイドリスク）と、「ITの利活用に伴う企業価値の向上」（アップサイドリスク）に特に着目した概念として理解される必要がある」[*1]として、ITガバナンスをコーポレート・ガバナンスの一側面として捉えている。

これに対してIT管理は、「部門ごと又はプロジェクトごとに、ITの利活用に関する「P（計画）－D（実施）－C（点検）－A（是正・改善）」の管理サイクルをまわすことによって行われる現場レベルでの活動である」[*1]とされており、「企業のさまざまな管理活動を実効ならしめるためには、取締役及び監査役における効果的なITガバナンス機能の発揮が不可欠となってきている」[*1]として、IT管理がITガバナンスの下で行われるべきとしている。

解説

ITガバナンスを特別視することなく、他のコーポレート・ガバナンスに関わる活動と同様に、ITリスクについてもダウンサイドリスクとアップサイドリスクの2つの観点から対処する必要があるということである。

ITに関わるダウンサイドリスクの例としては、システムの停止が損失につながるリスクであるとか、情報漏えいによって社会的信用が失墜するリスクなどがあり、アップサイドリスクの例としては、新規事業の立ち上げを実現するためのシステム導入や、ステークホルダーに対する適時適切なリスク情報の開示による市場からの信

頼の獲得などがあげられる。

なお、アップサイドリスクへの対応においてもダウンサイドリスクの検討が必要となる、あるいはダウンサイドリスクへの対応が結果的にオポチュニティにつながることもあるという点にも留意すべきである。

例えば、アップサイドリスクへの対応としてシステム統合によって企業再編の効果を高めようと考えた際に、早急に結果を求めて無理な導入スケジュールを立て、十分な品質管理ができなければ、プログラムバグが残存したまま利用開始され、結果的に重大なシステム停止や誤動作を招いてしまうかもしれない。逆にダウンサイドリスクへの対応としてアプリケーションシステム開発時にセキュリティや保守性、拡張性などに十分考慮した設計を行った場合、当該システムを長期間にわたって安定的に利用できるだけでなく、パッケージソフトウェアに改良して外販することで収益に貢献できることもある。

4. ITガバナンスの重要性と監査役としての関わり方

ITガバナンスにおける取締役と監査役の役割と責任に関して本報告書では、「取締役は、ITリスクを技術的に捉えるのではなく、当該リスクが顕在化したときの企業経営に与える影響を想定しておく必要がある。したがって、監査役は、取締役がITリスクの管理・対処を現場任せにせず、企業経営に対する影響という大局的視点から経営リスクとして認識・把握しているかどうかを監視・検証することで、ガバナンスの機能を発揮すべきである」[*1]と述べている。

そして取締役が経営リスクとして対処すべきITリスクとして、システムの停止や誤動作あるいは情報漏えいなどの不正行為によって「大きな損失を招くリスク」、「法令違反を犯すリスク」、また事業戦略の観点からITが「事業戦略を達成できないリスク」やITに関わる「投資の失敗を招くリスク」、加えて業務活動レベルで「業務活動の有効性と効率を著しく損ねるリスク」と「事業・業務継続に致命的な影響を及ぼすリスク」があるとしており、これを受けて「監査役は、ITリスクをもって「取締役が対処すべき重要な経営リスク」という観点で捕まえ、大所高所から、取締役の職能と責任を監視・検証することを通じてガバナンス機能の発揮が求められる」[*1]としている。

解説

ITガバナンスの中核となる経営リスクとしてのITリスクへの対応は、一義的には取締役の役割であり、取締役には全社的なリスクとしてのITリスクを識別し、その対処として企業あるいは企業グループ内にIT管理を確立することや、外部のステークホルダーに対して必要な情報を開示することなどが求められている。

したがって、このような取締役の職務が適切に執行されているかどうかについて、独立した視点で監視、検証することで取締役の職務を牽制し、取締役に対して一定の規律付けを行うことが監査役に求められる役割である。

本報告書ではQ&AのQ1の回答中に「このようなことが取締役会で議論されているかどうかを厳しく監視し検証するだけでも取締役に対する牽制」[*1]となると述べられており、まずは前述の経営リスクとして対処すべき6つのITリスクについて取締役が認識し、適切に対処しているかを監査することが有効としているが、より「厳しく監視し検証する」ためには、単に取締役会においてITリスクについて議論されているか否かという手続的な観点にとどまらず、どのような事象あるいは課題が経営リスクとなるITリスクに関係するかを監査役自らも意識し、より的を絞った監査を行うことで、取締役に対してより効果的に牽制をかけていくことが望まれる。

5. 監査役から見たITガバナンスとはどのようなものか

5.1 ITガバナンスとは何か

本報告書は監査役に向けて書かれているため、監査役の職能と責任を反映した形で、ITガバナンスについて次のように定義している。

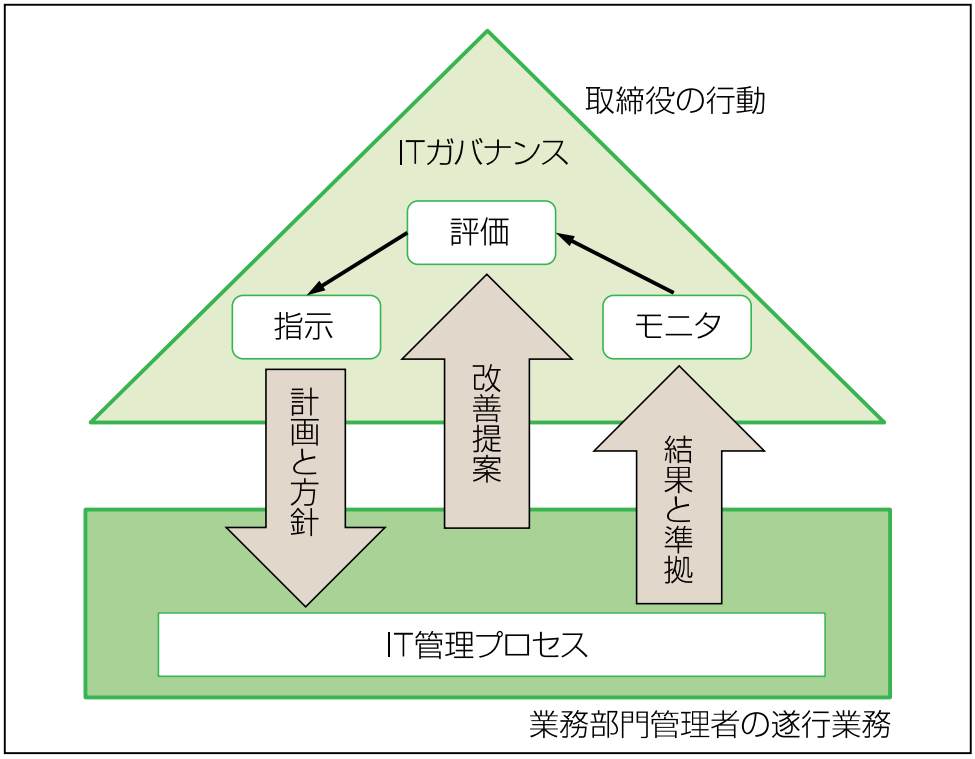
「ITガバナンスとは、コーポレート・ガバナンスの一側面であって、企業価値の向上を目指しつつ企業の社会的責任を果たし、かつ事業継続と業務の有効性及び効率性を達成するために、ITの戦略的利活用とそれに伴うリ

スクに対して、全社的に対処するための取締役の職能と責任の明確化、及びそれを独立した立場から監視・検証する監査役の職能と責任を通じて、企業グループ全体としてのIT利活用の適切な推進とIT利活用をめぐるリスク対処を効果的にするための仕組みないしは活動をいう。」[*1]

解説

ここではまずITガバナンスの主たる担い手である取締役がITの戦略的利活用とリスク対応に関して主に何をすべきかという点について、その概要を理解するため、「ISO/IEC 38500:2008 Corporate Governance of Information Technology」のITガバナンスモデルをベースに説明する。なお、本報告書におけるITガバナンスの全体像については後述5.4項にて改めて解説する。

図表1：ITガバナンスとIT管理の関係



参考：ISO/IEC 38500:2008

図表1では、上に描かれたITガバナンスという三角形と太い矢印が取締役のとるべき行動、その下のIT管理プロセスという四角形が業務部門管理者の遂行すべき業務を示している。

図ではまず取締役がITの現状および将来の利用を評価して企業としてのIT戦略を決定し、その達成のための計画と方針を業務部門に指示することで、これに基づき業務部門の管理者がいわゆるPDCAサイクルに則ってITプロジェクトやIT業務運用といったIT管理を実施し、その結果報告をもとに取締役が達成状況と方針への準拠をモニタリングし、また業務部門からの提案も含めてIT戦略と方針を再評価するという関係が示されている。

これがITの戦略的利活用とリスク対応に関して取締役が実施すべき活動であり、監査役による独立的監視、検証を通じた規律付けとあわせてITガバナンスを構成している。

5.2 ITガバナンスが目指すもの

本報告書では、ITガバナンスの目的を外部のステークホルダーを意識した対外的目的と、企業内部のリス

クへの対応という対内的目的に分類したうえで、前者として「企業価値の向上」と「社会的責任の履行」、後者として「事業・業務継続の確保」と「業務の有効性と効率性の達成」の4つの目的を挙げている。さらにこれらの「目的は密接に関連し合って、ガバナンスとしての最終目的をなすものであって、それぞれの目的を切り離して単独で考えることは適切ではない」[*1]としており、それぞれの目的が相互に関係していることから、「これらの目的は一つのサイクルとして認識することもできる」[*1]と述べている。

対外的目的については、まず企業価値の向上に関して、「ITの戦略的利活用こそ企業価値の向上のカギを握っている」[*1]としたうえで、逆に「情報セキュリティ事故は企業価値を大きく損ねる可能性がある」[*1]として、その失敗が重大な経営リスクにつながると述べている。次に社会的責任の履行については、「ITリスクやその管理体制に関するステークホルダーへの情報開示、個人情報保護法等のITに関連する法令遵守、グリーンITの積極的な採用等に向けた対応が求められている」[*1]、特に「情報開示は、事後的な説明責任の履行に留まらず、情報の事前開示によるステークホルダーの意思決定有用性の向上と、情報開示による取締役の規律付けという目的が加わってきている」[*1]として、社会的責任の履行が企業の重要課題となっていると述べている。

続いて対内的目的に関しては、事業・業務継続の確保について、「情報システムの機能停止や誤動作の未然防止は、事業・業務活動の有効かつ効率的な運用にとって不可欠なものである」[*1]と述べており、最後の業務の有効性と効率性の達成に関しては、「先に情報システムありきではなく、社内業務の何をどのように改善するのかということが明確になっていなければならない」[*1]と述べている。

解説

ITガバナンスの4つの目的について、その達成に向けて考慮すべき点を例を交えて解説する。

まず企業価値の向上と、業務の有効性と効率性の達成の2つの目的に関わる例として、経営戦略の達成のために新システムを導入することを考えてみる。この場合、経営戦略を明確に定めたうえで、その実現のために業務をどのように改善、デザインし、その中でITをどのように利活用すべきか詰めていくというプロセスが重要である。これは画期的な新技術を導入する場合であっても、パッケージソフトウェアを利用する場合であっても基本的に同じであり、このような検討を経ずに単に新しいテクノロジーを導入しただけでは戦略目標の達成はおろか、既存業務の効率低下や業務部門の混乱などを招いてしまいかねない。例えば他社で導入しているITソリューションが何となく良さそうだからといって、自社にマッチしないITを導入すれば投資の失敗、ひいては企業価値の低下につながることもあり得る。

次に企業の社会的責任の履行であるが、これにはITリスク管理に関する情報開示やコンプライアンスなどが含まれる。企業のIT利用に関係する法令は多岐にわたっており、金融商品取引法における内部統制の評価と監査であるとか、個人情報の保護に関する法律、不正アクセス行為の禁止等に関する法律、著作権法、不正競争防止法、あるいはデータセンタに関する建築基準法や消防法、また派遣労働に関する労働者派遣法などがあり、海外に子会社を有する場合には現地当局の法令についても対応が要請されることになる。コンプライアンス違反やステークホルダーに対する説明責任が果たされない場合には、罰則が適用されたり損害賠償請求が発生するといった直接的影響にとどまらず、企業イメージや信頼が毀損されることで、場合によっては企業活動の持続が困難なものとなってしまうこともあり得る。

事業・業務継続の確保については、本報告書では「情報システムの機能停止や誤動作の未然防止は、事業・業務活動の有効かつ効率的な運用にとって不可欠なものである」[*1]と述べているが、実際には未然防止できずに情報システムが停止し、業務遂行に必要なITサービスが継続できなくなることもあり得るため、その要因について予めリスク評価を行い、バックアップの取得やデータセンタの防災対策などの事前対策と、復旧体制の構築、運用や事故後の適切な情報開示といった事後対応についても計画を策定しておくことが重要といえる。

5.3　ITガバナンスを構成する要素とは

本報告書では次の5つの構成要素を一連のチェーンと

して捉えるべきと述べている。

① ITの利活用をめぐる組織風土の健全性の確保とその監視
② 経営戦略としてのIT戦略の明確化とその監視
③ 経営リスクとしてのITリスクの評価とその監視
④ IT管理方針・体制の整備とその監視
⑤ IT管理プロセスの定期的チェックとその監視

ここで監視というのは取締役による相互監視と監査役による独立的監視・検証を指している。

解説

上述の5つの構成要素において取締役が直接的に達成すべき事項としては、「･･･とその監視」の前に書かれた事項となる。

このうち、②から⑤については基本的に5.1項の図表1で示した「評価ー指示ーモニタ」というサイクルを通じて行う活動と対応しており、そのポイントは②・③に示されているように、IT戦略あるいはITリスクを経営戦略、経営リスクとして捉える点にある。

5つの構成要素のうち、残りのひとつ、すなわち①の「ITの利活用をめぐる組織風土の健全性確保」は、実際にITの利活用を行う「人」に着目したものであり、組織構成員のITリテラシーの一環として、特にセキュリティやコンプライアンス意識の向上により、組織としてITリスクに適切に対応できるような風土、カルチャーを醸成し、定着させていくことを指している。なお、ISO/IEC 38500においても、「良質なITガバナンスのための6つの原則」の中で、

「原則1　責任　組織内の個人及びグループがITのための供給及び需要の両方の点で彼らの責任を理解し受け入れる。」*2

「原則6　人間行動　ITの方針、実施及び決定は人間行動を尊重している。」*2

という2つの原則を提示しており、実際にシステムを利用し、業務を遂行する「人」の意識と行動を考慮することが重要であると指摘している。

これら「人」あるいは組織風土に関する課題は、組織構成員に対する教育の実施、あるいはセキュリティやシステム利用に関するルールの整備と徹底、また問題発生時の報告体制の導入などによって形作られていくものであるが、このような体制整備を形式的な一過性のものとせずに、上述の②から⑤のサイクルを着実に回していくことで定着を図るとともに、組織構成員のマインドを高めていき、その結果としてより健全な組織風土を育んでいくことが重要といえる。

5.4 ITガバナンスの全体像（フレームワーク）

本報告書では監査役の取締役に対する規律付けについて、「ITの利活用に関する取締役の職務執行とその相互監視を、監査役が独立的な立場から監視・検証し、取締役の独断暴走や相互監視の馴れ合いを防ぐことで、ガバナンスの機能が達成できるという構造で理解されなければならない」*1としており、またステークホルダー、会計監査人、IT管理およびIT内部監査担当との関係について、次のように説明している。

① ステークホルダーとの関係

「ITガバナンスに関する取締役としての役割と責任の履行状況は、（中略）、外部ステークホルダーに対して適切かつ適時に開示されるべきであり、ステークホルダーからの指摘・提言も取り入れられるような仕組み作りが肝要である。」*1

② 会計監査人との連携

「監査役は、会計監査人との連携を保ち、とりわけIT化されている業務プロセスに係る内部統制の評価については、監査上の着眼点についての説明を受けるなどして、適切な監査手続が採用されていることを確認しておく必要がある。」*1

「このような会計監査人との連携は、法令上定められた監査役の任務遂行という意味の他にも、監査役が行う監査業務の有効性と効率化を高める観点からも重要である。」*1

③ IT管理との関係

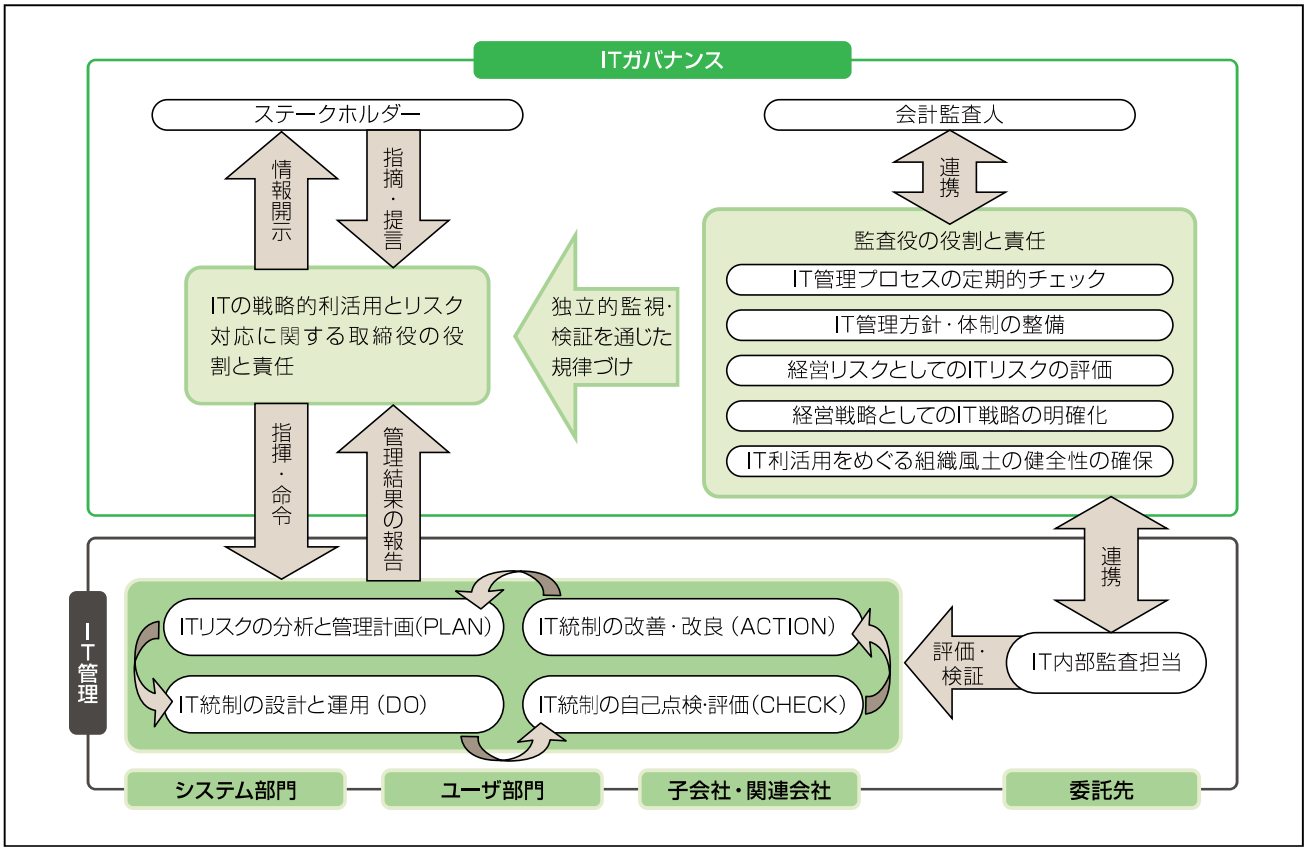
「取締役の役割と責任に基づいて、指揮・命令を通じて管理者層の活動としてのIT管理へとブレークダウンされ、またIT管理の結果は定期的に（突発事象が発生した場合には適時に）取締役に対して報告されなければならない。」*1

④ IT内部監査担当との連携

「部門管理者層が担うIT管理の評価・検証は、取締役のスタッフ機能を果たす内部監査部門が実施し、内部監査報告書を通じて取締役にその結果が報告される。」[*1]

「ITガバナンスの機能がIT管理に生かされていることを確認するためにも、監査役は内部監査担当と定期的に意見交換し、内部監査報告書の写しを入手するなど、連携を保っておくことが効果的である。」[*1]

図表2：IT管理との関係を踏まえたITガバナンスの全体像



出典：日本監査役協会 ITガバナンス研究会「監査役に期待されるITガバナンスの実践」、平成23年8月25日

解説

まず、図表2の左上に描かれている「ITの戦略的利活用とリスク対応に関する取締役の役割と責任」の構成要素は、「監査役の役割と責任」に記載された5つの構成要素と同様であり、取締役がその推進を担い、監査役が独立的監視・検証を通じて取締役の職務を規律付けることを表しており、ITガバナンスの核となっている。

次に取締役の役割と責任の観点から、対外的なステークホルダーとの関係と、対内的なIT管理との関係について解説する。

まず、外部のステークホルダーとの関係は、5.2項で述べたITガバナンスの4つの目的のうちの対外的目的である「企業価値の向上」と「社会的責任の履行」の達成に深く関わる事項である。ITが企業活動において広範に利活用されている現在においては、間接的なものも含めて企業のITとステークホルダーとの接点は多岐にわたっていることから、これらを踏まえて株主や取引先、顧客などに対する社会的責任への取組みの一環として、適切に情報開示や対話などのコミュニケーションを促進していくことが重要となっている。具体的にはインターネットの企業サイトにCSRレポートを掲出して質問や意見を受け付ける、ステークホルダーへの説明会や意見交換会を開催するなどさまざまな方法があるが、より詳しくは経団連が発行している「企業行動憲章 実行の手

引き」や「ISO26000:2010 Guidance on Social Responsibility」などを参照頂きたい。

IT管理については、5.1項で述べたように、取締役がIT戦略を決定し、そのための計画と方針、もしくはそれらの立案を業務部門に指示し、これに基づいて業務部門でIT管理のPDCAサイクルが実行され、結果がモニタリングのために取締役に報告されるという関係がある。この報告には定例的なシステム運用状況報告やプロジェクトのマイルストーン毎の進捗報告、突発事象に関する緊急報告などが含まれるが、それらは取締役がITガバナンスの観点で必要な情報、すなわち経営リスクの視点でなされることが望まれる。したがって、報告すべき事項と内容、タイミングについてITリスクの管理方針として予め定めるとともに、この方針をIT管理を担当する業務部門に対して周知して、適切な報告が適時に行われるようにしていくことがポイントとなる。

続いて監査役と会計監査人との関係であるが、監査役は会計監査人との間に、独立しつつ協力、連携することが求められていることから、会計監査人が実施するITに関わる内部統制の評価手続や結果に依拠する、あるいは利用するなどして効果的で効率的な監査を計画、実施することがポイントとなる。ただし、会計監査人が実施する手続の目的や範囲は、例えば金融商品取引法に基づく内部統制の監査が財務報告に関するものに限定されているように、監査役監査で求められているものとは異なる点に留意しなければならない。

最後に監査役とIT内部監査担当の連携であるが、内部監査は業務管理状況に関する評価、検証を行い、取締役に報告する職務を担っていることから、IT管理についてもリスク対応手続として、ITリスクとコントロールに関するPDCAサイクルが適切に回っていることを監査する。したがって、監査役がIT管理に関わる内部統制の導入と運用状況を確認する、あるいは監査役監査としてIT管理に関してどこに焦点を当てた計画を立案するか検討するうえで、IT内部監査担当との情報交換が有効といえる。

6. 結びに代えて

経営層が対処すべきITリスクは経営リスクとしてのITリスクであり、ITガバナンスの目的として挙げられている企業価値の向上や社会的責任の履行、事業・業務継続の確保、あるいは業務の有効性と効率性の達成を阻害する要因を的確に把握して対応することが求められている。

ここで悩ましい点のひとつに、経営リスクとしてのITリスクの評価は、現場のIT管理レベルにおける個別的なITリスク評価とは目的や観点が異なるとはいうものの、ITが企業において広範に利活用されている現状では、個別的なITリスクがしばしば経営インパクトのあるリスクにつながっていくという点がある。

そのようなITリスクを経営層が認識、対処していくためには、本報告書で述べられているようにすべての取締役がITリスクの認識を共有することが必要であるが、加えてIT管理レベルのリスク管理結果を経営視点で整理して取締役に報告することも有効と考えられる。

経営リスクの視点でITリスクの報告が上がるようになれば、リスクの影響や対処優先度などの判断がしやすくなり、取締役が速やかに次の手を打てるようになることが期待できる。

このようなITガバナンスとIT管理の連携をサポートする概念として、GRC（Governance, Risk and Compliance）という統合的リスク対応の考え方があり、そのための手法やツールが整備されてきている。今後、これらを適切に利用してITに関するガバナンス、リスク、コンプライアンスが統合的に対応されるようになれば、経営者の指示によって管理者が実施したITリスク管理の結果をダッシュボードを通じて大局的視点で把握できるようになるなど、ITガバナンスの有効性と効率性の改善に貢献することが期待されている。

参考資料

＊1. 社団法人日本監査役協会.《ITガバナンス研究会報告書》監査役に期待されるITガバナンスの実践. 2011. ページ: 1-20. http://www.kansa.or.jp/support/IThoukokusyo.pdf

＊2. ISO/IEC38500:2008. Corporate governance of information security. 2008.