protiviti®
Risk & Business Consulting.
Internal Audit.

Risk Oversight vol.27
取締役会のリスク監視

ITリスクを監視する

IT技術の息をのむような発展は社会のあり方を大きく変え、IT技術相互間で影響しあっています。ITを活用することで企業はコストの削減、ビジネスプロセスの改善、そして収益の拡大を計っています。ITはいまや企業の質的変化の源泉そのものです。

主要な考慮事項

200名以上の企業取締役を対象に実施された最近のサーベイ(*1)によると、対象取締役のうち47パーセントは自社の取締役会のITリスクを監視する能力は不十分だと回答しています。このサーベイ結果は、従来は投資予算の承認の一部として、個々のITプロジェクトの評価に限っての取締役会のリスク監視をより広く捉えなおす必要を示しています。

以下の項目は、取締役会がITリスクをより広い視点から監視する上で念頭に置くべき事項です。

- **まずはじめに意識しなければならないこと**

  取締役がITリスクを監視する上でまず意識しなくてはならないことは、「そもそもどのような内容のリスクがあるのか」「どのようにリスクを管理しているのか」「どのようにリスクが管理されていることを確認しているのか」の3点です。これらの疑問を通じ、取締役会はITリスクは他のビジネスリスクの一部であると同時に、全社的に評価すべき特定のリスクでもあることを認識しなければなりません。

- **統合的・大局的なアプローチをとる**

  取締役会は、ITリスクを付随的な項目として考えるのではなく、戦略リスク、オペレーションリスク、財務リスク、コンプライアンスリスクと統合して監視しなければなりません。例えば、戦略リスク・財務リスクにはIT技術の革新、リソースの配分、プロジェクトマネジメントに伴うITリスクが関連しますし、オペレーションリスク・コンプライアンスリスクには機密情報の保持、セキュリティ・プライバシー、ITリソースの可用性、ITサービスへのコスト配分やインフラリスク等の内部プロセスリスクが関連します。なかでもセキュリティ・プライバシー漏洩やIT業務の中断が特に重大なリスクですが、他のリスクも無視できません。

- **ITリスクの監視に適した体制を構築する**

  ITを監視する役割は監査委員会が担う場合が多いようですが、監査委員会の焦点が財務報告・財務統制関連に限定されてしまう例も多く見られます。取締役会の経営戦略の策定ならびに執行の監視方法に照らして、監査委員会の代わりに独立した経営戦略委員会や財務委員会において戦略的IT事項を評価することも考えられるでしょう。企業の戦略の持続性におけるITの重要性によっては、独立したIT委員会を設置してもよいかもしれません。また、独立したリスク委員会を設置している場合は、同委員会で担当することも考えられます。

- **ビジネスモデル上のITの役割を理解する**

  戦略的サプライヤー、チャネルパートナー、顧客や調達先との間でITを用いて結びついている企業においては、取締役は、経営者に対しITを統合したビジネスの構図を示すように求めなければなりません。

- **ITリスクにはコンプライアンスの側面もあることを忘れずに**
  業種を超え、新規の法規制ならびに法改正が継続的に進んでいます。コンプライアンス違反は厳しい結果をもたらしかねません。したがって、法の要請を満たす上でもITの活用が必要となります。
- **内部監査を強化する**
  プロティビティの2011年版IT監査サーベイによると、対象となった監査担当者500名のうち、20パーセントはIT監査機能がそもそも存在せず、16パーセントはIT監査に関するリスクアセスメントを実施しておらず、42パーセントはITリスクを評価するのに必要なリソース・能力が不足していると回答しています。
- **取締役会の意識を高める**
  ITリスクの監視のためには大半の取締役会は、より高い知識や意識が必要です。この点についてはCEO、CIOや経営戦略責任者の補佐を活用すべきです。

取締役会の考慮事項

以下は自社の遂行するビジネスに伴うITリスクの性質に応じ、取締役会が考慮すべき事項です。

- 取締役会はITリスクおよびそれを管理するプロセスを監視するのに十分な時間を費やしているか。
- 自社は競合他社（および自社従業員）が新しいテクノロジーをどのように活用しているかを含め、IT技術の革新を監視しているか。老朽化したシステムが効率性・敏捷性・イノベーションを阻害していないか。
- 個々のITプロジェクトが、将来において、どの程度費用削減やビジネスプロセスの改善、戦略目標の達成等の効果をあげるかについての前提を理解し、またその達成度をどのように測定するかについて理解しているか。大型プロジェクトが目的を達成していることを確認するためのフォローアップを実施しているか。
- 取締役会は（1）自社のIT費用全体および（2）投資効率を最適化し、法規制・契約上の要請を満たすために、プロジェクト全体に占めるIT費用が適切であるかについて十分な情報を得ているか。
- 取締役会は自社の直面している情報プライバシーやセキュリティリスクを理解しているか。新しいビジネスプロセスにおいても情報プライバシーやセキュリティは検討されているか。
- CIO・情報管理部門は事業の変化に即したサポートを十分に提供しているか。
- クラウドソリューションを利用しているか。利用している場合、取締役会はクラウドに関連するリスクを理解しているか。
- アウトソースを利用している場合、取締役会はアウトソース先との関係が十分管理されているか確認しているか。
- 取締役会は企業・業種に関連するIT事項について精通しているか。

プロティビティの支援

プロティビティは、情報システムの投資効率の最大化、ITリスクの最小化、ITインフラの効率化に関する支援を実施しています。プロティビティの幅広いITコンサルティングサービスはITビジネスマネジメント、ITセキュリティとプライバシー、アプリケーションとデータ等、多岐にわたります。また、プロティビティのベンチマークサービスは経営者がITをビジネスの要件と統合し、費用効率の高いIT組織の実現を可能にします。

プロティビティについて

プロティビティ（Protiviti）は、リスクコンサルティングサービスと内部監査サービスを提供するグローバルコンサルティングファームです。北米、日本を含むアジア太平洋、ヨーロッパ、中南米、中近東において、ガバナンス・リスク・コントロール・モニタリング、オペレーション、テクノロジ、経理・財務におけるクライアントの皆様の課題解決を支援します。
プロティビティのプロフェッショナルは、経験に裏付けられた高いコンピテンシーを有し、企業が抱えるさまざまな経営課題に対して、独自のアプローチとソリューションを提供します。現在、世界の70を超える拠点で約2,500名のコンサルタントが活躍しています。

＊1　Taming Information Technology Risk : A New Framework for Boards of Directors、National Association of Corporate Directors and Oliver Wyman, 2011, 5頁　http://www.nacdonline.org/files/Taming%20Information%20Technology%20Risk%20Final.pdf

protiviti®
Risk & Business Consulting.
Internal Audit.