protiviti®
Risk & Business Consulting.
Internal Audit.

Risk Oversight vol.67
取締役会のリスク監視

取締役会にIT事項を説明する

取締役はIT事項についての説明を受ける際に、メッセージを完全に理解しているでしょうか。あるいは、メッセージはあまりにも複雑で理解できないものでしょうか。以下では、取締役会に対してIT事項の説明を行うにあたっての3つの関係について論考します。それぞれの関係は、最高情報責任者（CIO）と最高情報セキュリティ責任者（CISO）が説明内容を整理する上で、また取締役が得るべき情報に対する方向性に関する洞察を提供します。

今日の環境において、多くの企業は、それらのビジネスモデルがテクノロジなしでは機能しえないことから、実際には「テクノロジ・ビジネス」であると言えます。革新的なテクノロジは、市場において差別化をもたらす要素であると同時に、破壊をもたらす要素でもあります。テクノロジの進歩によって、ビジネスモデルの価値が半減するまでの時間は急速に短くなっています。これまではテクノロジに依存すると考えられていなかった産業は、今テクノロジによって変質しつつあります。テクノロジの影響を受けない企業はほとんど存在しません。例として、ロンドンのタクシーやウーバー（Uber）が挙げられます。オンライン予約や、モバイルデバイスによってタクシーの現在位置を把握し、どこからでもタクシーを呼び、ユーザー登録情報を管理できることは、重要な差別化要素です。結論は、テクノロジはもはや単なる手段ではないということです。

取締役から、組織が直面するITリスクに関する自身の理解が十分ではないとのフィードバックを受けることがよくあります。このフィードバックは、プロティビティが開催したラウンドテーブルやお客様の会社の取締役との対話から得られたものです。

全米取締役協会が行った2013～2014年の公開会社ガバナンス・サーベイによると、取締役が経営者から提供を受ける情報の中で、ITは質と量の両面で最も満足度が低い分野とされています。

取締役会はITが重要な企業資産であることを理解する必要があり、ITに関連する機会やリスクは取締役が理解できるような方法で伝達されなければなりません。取締役はITリスクがその重要性を増していることを直感的に認識しています。ソーシャル・ビジネス、クラウド・コンピューティング、モバイル・テクノロジやその他の進展は、費用対効果に優れたビジネスモデルを創造し顧客体験を高めるための重要な機会を提供します。それらはまた、破壊的な変化や、プライバシーとセキュリティに関するより大きなリスク、サイバー攻撃に対するより多くのエクスポージャーを生じさせる可能性があります。

これらの変化によってもたらされる新たな課題は、実際において、会社が管理すべき目標が“移動し続けている”という状況を作り出しています。新たなテクノロジによる破壊的革新の速度は突発的な災害ほどではありませんが、影響の持続性という意味では、変化に乗り遅れた組織にとっては致命的となる可能性があります。

また、CIOとCISOの取締役会（ドイツのように二層制が採用されている場合にはスーパーバイザリー・ボード）との関係は変わり続けています。これらの動向は、現在および将来においてCIOやCISOが取締役会に対して説明を行う際に直面する環境や期待を要約するものであり、取締役会との意思疎通をビジネスモデル、戦略、および／あるいはリスクとの関係において位置付けるものです。

主要な考慮事項

多くの組織において、CIOとCISOは少なくとも年に一度、ITに関する状況について、全員が出席する取締役会あるいは監査委員会への説明を行っています。以下は、この説明を行うにあたっての3つの方法です。

- **事業との関係において説明を行う**—CIOあるいはCISOは、商品やサービスの市場への提供においてビジネスモデルがどのようにテクノロジを活用しているかや、破壊的な変化から生じる機会とエクスポージャーについて説明を行います。事業と関係づけて説明を行うことにより、以下のような質問に対する回答が提供されます。

  1. 当社は破壊的な可能性を持つテクノロジの業界レベルでの進展について理解しているか。新たなテクノロジを適時にビジネスに組み入れることができるよう、変化を十分に先取りしているか。
  2. 新たなテクノロジが、事業目標を達成するために効果的に導入されているか（例えば、顧客ロイヤルティの達成、品質改善、時間短縮、コストとリスクの削減、および技術革新の推進など）。
  3. 当社の業務は、持続的な競争優位を確保するために必要な革新的変化を予測し、プロアクテイブに革新を推進しているか。
  4. 事業活動を行うバリュー・チェーン内において、競争の状況や顧客の期待、戦略的なサプライヤーおよび／あるいは流通チャネルとの関係を変えうる新たなテクノロジは何か。現行の業務やテクノロジの破壊的な変化に対してエクスポージャーはどの程度であり、予測可能な将来における事象によってどの程度その有用性が限定されているか。
  5. テクノロジに関する能力について、アナリストや株主、一般公衆との対話において共有すべき側面があるか。そうであれば、その共有が行われているか。共有が行われていないのであれば、それはなぜか。

- **戦略の実行との関係において説明を行う**—CIOあるいはCISOは、戦略的イニシアティブが如何にして重要なテクノロジによって推進されているかや、それらの様々なテクノロジの有効な機能を確保するためのコントロールの整備と実施を組織がどのようにして促進しているかについて、明確な説明を行います。戦略の実行との関係において説明を行うことにより、以下のような質問に対する回答が提供されます。

  1. 戦略的イニシアティブの実行において重要なテクノロジは何か（例えば、成長、利益の改善、技術革新とプロセスの改善など）。
  2. これらのテクノロジの有効な機能をどのように確保しているか。
  3. 組織がこれらのテクノロジに対して行う投資への適切なリターンの実現を確保するために、IT部門と事業部門はどのように協働しているか。
  4. 戦略を実行するためにこれらのテクノロジを導入する上で、どのような課題に直面しているか。これらの課題は、戦略的イニシアティブの成功にどのような影響を与える可能性があるか。
  5. 戦略的イニシアティブを実行するために必要な信頼性と適時性のある情報とデータを入手しているか。

- **リスク低減との関係において説明を行う**—CIOあるいはCISOは、事業に対するより広い視点で、テクノロジから生じる可能性のある特定のリスクや、テクノロジの利用によって部分的に低減される特定のリスクを識別します。リスク低減との関係において説明を行うことにより、以下のような質問に対する回答が提供されます。

  1. ITから生じる最も重要なリスクは何であり、それらのリスクがレピュテーションやブランドイメージを含む事業にどのような影響を与えるのか。これらのリスクに対する許容度を評価しているか。
  2. 重要なリスクを受容できる水準まで低減しているか。低減できていると考える根拠は何か。

3. 重要なテクノロジコンポーネントに依拠したリスク対応によって低減している重要な事業リスクは何か。このテクノロジコンポーネントは有効に機能しているか。有効に機能していると考える根拠は何か。

目的は、上記の3つの関係の全てにわたって取締役と共感できるIT事項に関する説明を行うことにあります。

1. **事業との関係：**破壊的な変化を管理しているか。
2. **戦略との関係：**寄与する価値ならびに投資に対するリターンを最大化しているか。
3. **リスク低減との関係：**リスクが事業とレピュテーションに与える影響を管理しているか。

上記の論考は次の2つの恒久的な原則に基づいています:(1) 事業目標はITの目標でもある、そして (2) ITリスクは事業リスクを意味する。これらの原則を用いることにより、上記の事業、戦略、およびリスク低減との関係を踏まえた視点は、CIOにどのように取締役会と対話すべきかについての洞察を与えるとともに、取締役にCIOから期待すべき情報が何であるのかについての洞察を与えます。

てきぱきとして、専門用語を用いずに、上記の事業、戦略、およびリスク低減との関係に触れ、それらとの関係における問いに答えることにより、取締役会との継続的な対話を促進することができるでしょう。この点に関して、CIOあるいはCISOは以下の事項を行うべきです。

- **事業を理解していることを示す**—上記3つの適切な関係を用いて、関連性のあるIT関係の目的、目的を達成するための計画、計画を実行するための組織的能力、および進捗を測定する方法まで掘り下げを行います。今日の世界において、テクノロジはその革新を通じて事業の変革と成長を促進しますが（事業との関係）、十分な保護とコントロールが行われなければレピュテーションを破壊してしまう可能性もあります（リスク低減との関係）。取締役には、相互に関連する上記の関係の双方について助言を求めるべきです。

- **取締役会のニーズに焦点を当てる**—取締役会は、CIOあるいはCISO管轄部門の運営と管理がどのように行われているかについての詳細を知りたいとは考えていません。求められない限りは、そのような説明を行う必要はありません。

- **IT面での影響や尺度だけではなく、事業面での影響や尺度について説明を行う**—事業の全体を視野に入れ、事業への影響に焦点を当てる必要があります。例として、「当社のシステムの99パーセントは10日以内に修復可能」という尺度が挙げられます。この尺度は、データのセンシティビティや残り1パーセントのシステムの障害が事業に与える影響についての問いには答えていません。

- **聞き手に照準を定める**—取締役会に対する説明の目的を理解することが重要です。取締役会議長に説明の方向性を確認する必要があります。また、取締役会に対して説明を行ったことがある人々から、様々な取締役の経歴や性格について情報を得るべきです。

- **簡潔で要を得た説明を行う**—取締役は全ての情報を欲しているわけではありません。取締役が知る必要のある事項に焦点を当て、それ以上の説明を行う必要はありません。複雑なナレッジは注意深く共有すべきです。取締役が記憶に留めるべき事項を特定し、それらの事項の重要性を説明することが必要です。質問を受ける時間も確保すべきです。午後の遅い時間に取締役会への説明が予定されている場合には、説明を手短に行うように求められる可能性があることを念頭に置く必要があります。

取締役会は、CIOとCISOに対する期待を明確にする必要があります。取締役のニーズ、取締役が理解していない事柄、そしてITにおける課題と関連する事業リスクのうち取締役にとって最も大きな関心事は何でしょうか。また、より重要な問いは、取締役はCIOやCISOに、何との関係においてIT事項について説明を行ってほしいのかということです。さらに、ITは元来複雑なものであることに鑑み、取締役のCIOやCISOに対する期待は現実的である必要があります。このため、説明に割り当てられた時間は、取締役の説明に対する期待と釣り合いが取れているべきです。

取締役会の考慮事項

以下は、事業体の活動に内在するリスクに関連して取締役会

が考慮すべき事項です。

- テクノロジがもたらす機会と破壊的変化を主導および／ないしは破壊的変化への対応を行う可能性は、戦略策定プロセスにおいて考慮されているか。あるいは、テクノロジは単に戦略実行の手段としてより狭義に捉えられているか。

- 取締役会は、関連する機会とリスクを含むIT事項や、それらの機会とリスクを管理する上での組織の能力とプロセスについて、十分な時間を割いているか。

- 取締役会はCIOとの定期的なコミュニケーションに満足しているか。そうでなければ、今後のコニュニケーションが的を射たものになるよう、取締役会はCIOに取締役会としての期待を伝えているか。

- CIO組織は、変化し続ける事業のニーズを効果的に支援し、かつ競合他社（あるいは従業員）が破壊的な変化を生み出すために新たなテクノロジをどのように展開しうるかも含めたテクノロジの革新状況を有効に把握しているか。CIOは取締役会がこれらの課題を理解する上での助けとなっているか。

- 組織が直面するサイバー脅威が増加する中、取締役会はインシデント対応の準備度合いについてCISOと積極的な対話を行っているか。

- 重要なITプロジェクトについて、取締役会は、個々のプロジェクトがどのように戦略的目標を達成するのかについての基本的な想定や、プロジェクトの成功尺度を理解しているか。個々の重要なプロジェクトが予定どおりの成果を達成するようフォローアップは行われているか。

プロティビティの支援

プロティビティは、情報システム投資に対するリターンを最大化し、ITリスクを最小化するために、企業経営者を支援しています。事業戦略との整合性を確保するために強固なITガバナンスとプログラム管理プラクティスを活用することにより、プロティビティはITインフラを通じてエクセレンスを推進し、支援アプリケーションやデータ分析、セキュリティへと推進します。

プロティビティの包括的なITコンサルティングサービスは、お客様が優先順位の高い事業上の重要事項に対応する目的でテクノロジを活用するのを支援するために、以下の3つの主要領域をカバーしています。

- テクノロジ戦略と業務
- セキュリティとプライバシーに関するソリューション
- エンタープライズ・アプリケーションに関するソリューション

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、アフリカにおいて、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。

protiviti®
Risk & Business Consulting.
Internal Audit.