《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

平成 23 年 8 月 25 日

社団法人　日本監査役協会

はしがき

インターネット動画サイトへの内部情報の投稿、システム障害による為替の事務処理遅延や ATM 端末の利用不能、自社サイトへのハッカー攻撃による個人情報流出・・・・。この１年間に起こり、社会的に大きな影響があった情報セキュリティ事故の一部である。同様の事故が自社に降りかかったらどうなるのだろうかと慄然とされる監査役の方も少なくないのではなかろうか。

今日会社実務での IT の利活用は、会社の業務活動全般に及んでいる。IT の利活用は、企業の競争力の維持、向上を図る上で不可欠であるが、一方で、それに伴いリスクも増大している。場合によっては、経営の根幹を揺るがすような事態に陥るおそれもあるだけに、この増大する IT リスクに対し、会社としてしっかりとガバナンスを効かせていく必要がある。では、監査役としてはこの問題にどのように取り組めばよいのだろうか。

このような問題に対し、当協会では平成 13 年に IT ガバナンス委員会を協会内に設置し、IT 活用に伴う経営の変化への監査対応をテーマとして、「IT ガバナンスにおける監査役の役割」と題する報告書を作成し公表している（『月刊監査役』448 号、４－15 頁）。同報告書では、「事業活動のあり方にまで IT が影響を及ぼす現状から見て、監査役としても、その善管注意義務に反さないように、取締役が IT 化に対応した適切な処置を取っており、社内においてこれが適正に実施されていることを、モニタリングし、企業経営の健全性を確保していくことが強く求められるであろう」とした上で、いくつかのテーマを重点課題として取り上げ検討している。

その後 10 年を経て、企業における IT の利活用は、よりコアな業務に、より広範に及ぶようになり、その分リスクも高まる一方である。そこで、当協会では改めて、IT ガバナンスにおける監査役の今日的役割を検討すべく IT ガバナンス研究会を立ち上げ、その後の経営環境の変化も踏まえ、より実務に即した内容に改めるべく全面的にその見直しを行った。

IT ガバナンスという用語については、一般に、コーポレート・ガバナンスのうち IT 利用に関するガバナンス機能といった意味であるが、その時々の論点との関係からさまざまに使われ、未だ十分に成熟した概念にはなっていない。また、監査役監査との関係についても定説があるわけではない。しかし、当研究会に課せられたタスクとしてこれを捉えれば、検討すべきは、監査役の立場から IT ガバナンスをどのように理解し、どう取り組めばよいかを示すということであろう。そこで、当研究会として監

査役の立場からITガバナンスについて一定の定義を示し､それを基に検討を進めた。

本報告書は、次の２部構成となっている。

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

第Ⅰ部は、いわば総論部分であり、IT ガバナンスの重要性や必要性、その構成要素などを示し、まずは IT ガバナンスをどのように理解し、どのようなスタンスで取り組めばよいかの枠組みを示すことに重点を置いた。

第Ⅱ部では、IT ガバナンスの実現に向けて、最小限行うべきこと、最低限留意すべき事項に限定して、その取組み方のポイント等を示した。

情報通信技術の発展は依然目覚しいスピードで進展し、ソフトウェア、ハードウェアともに流行り廃りが激しい。また、IT の現場は、専門用語や特有の言回し、アルファベットの略語が飛び交う部外者には馴染みにくい部署でもある。これまで IT に縁の薄かった監査役の方にとって IT は、できれば敬遠したくなる事柄の一つであるかもしれない。

本報告書は、そのような監査役の方にとっても、すぐに監査の現場で活用できる内容とするため、できるだけ技術的な専門用語の使用を避け、また、監査役の実務に沿った多くの Q&A を盛り込んだ。皆様の監査実務にご活用いただければ幸いである。

なお、本報告書の作成にあたっては、専門委員としてご参画いただいた堀江正之日本大学教授に原案の起草や意見取りまとめに大変ご尽力いただいた。この場を借りて心から謝意を表したい。

IT ガバナンス研究会

委員長　広瀬　雅行

目　　次

［Ｑ＆Ａタイトル一覧］

*()*内は頁番号

［図一覧］

*()*内は頁番号

[主要参考文献]

ISO26000[2010] “Guidance on social responsibility”（日本規格協会訳「社会的責任に関する手引」）

ISO/IEC38500[2008] “Corporate governance of information technology”（日本規格協会訳「企業の IT ガバナンス」）

IT Governance Institute[2007] *IT Governance Implementation Guide: Using COBIT® and Val IT TM,* 2nd ed.（あずさ監査法人訳「IT ガバナンス導入ガイド 第２版」）

IT Governance Institute[2003] *Board Briefing on IT Governance*, 2nd ed.（ISACA 東京支部・日本 IT ガバナンス協会訳「取締役会のための IT ガバナンスの手引　第２版」）

Parent M. & Reich B.H.[2009] “Governing Information Technology Risk”, *California Management Review* , 51(3), pp.134-152

Selig,G.J.[2008] *Implementing IT Governance: A Practical Guide to Global Best Practices in IT Management*

Tarn,J.M.,et al. [2009] “ Exploring information security compliance in corporate IT governance”, *Human Systems Management* , 28, pp.131-140

鴻 常夫・江村 稔編集[2010]『監査役小六法　平成 23 年版』日本監査役協会

神田秀樹[2007]『会社法（第９版）』弘文堂

金融庁・企業会計審議会[2011]「財務報告に係る内部統制の評価及び監査の基準並びに財務報告に係る内部統制の評価及び監査に関する実施基準の設定について（意見書）」

経済産業省・情報セキュリティ政策室[2009]『情報セキュリティガバナンス』（財）経済産業調査会

日本監査役協会[2010]「有識者懇談会の答申に対する最終報告書」

堀江正之[2006]『IT 保証の概念フレームワーク』森山書店

堀江正之[2010]「監査役として IT システムにどう向き合うか」『月刊 監査役』575 号、58－67 頁

[委員名簿]

委員長	広瀬　雅行	㈱東京証券取引所グループ　取締役　監査委員
専門委員	堀江　正之	日本大学商学部　教授
委員	佐藤　益次郎	NEC モバイリング㈱　常勤監査役
委員	谷口　　明	協和発酵キリン㈱　常勤監査役
委員	松永　　望	㈱パイプドビッツ　常勤監査役
委員	水野　晴夫	㈱ワコム　常勤監査役
委員	渡辺　善子	日本アイ・ビー・エム㈱　常勤監査役
委員	宮本　照雄	(社) 日本監査役協会　専務理事

第Ⅰ部
IT 環境における監査役の役割と責任

１.IT ガバナンス概念登場の背景

IT ガバナンスという用語は、いわゆる企業不祥事の多発を受けたコーポレート・ガバナンス論議の高まりを受けて、1990 年代末から使われ出したものである。情報システムコントロール協会（ISACA）が、2000 年に、IT の統制と監査のガイド（COBIT という）において用いたことから普及しはじめた。

IT ガバナンスという用語が登場し普及した背景として、主に次のような点を指摘できるであろう。

- IT が企業の経営戦略や企業の価値向上と密接に結びつけられるようになり、取締役が IT の利活用に無関心でいられなくなってきたこと。
- IT が企業の業務活動に不可欠なものとなり、全社的にあるいは企業グループとしての有効かつ効率的な活用が必要となってきたこと。
- IT への投資では短期的な投資効率が優先され、セキュリティ投資が後回しとなりがちで、それが原因でセキュリティ事故を招くケースがあったこと。
- IT を利活用した情報システムの機能停止、IT を悪用した業務妨害や不正行為等の IT リスクが企業の事業継続･業務継続を脅かす重大なリスクとなってきたこと。
- IT が企業活動全般に浸透するようになり、IT リスクが情報システム部門単独で対処すべき技術的なリスクから、莫大な損失に結びつくリスク、法令違反につながるリスク、重要な顧客や取引先を喪失するリスク、業務の有効性と効率性を著しく損ねるリスク等々へとつながり、経営層（取締役及び監査役）による全社的な対応が必要な経営リスクとなってきたこと。

要するに、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」であると理解してよい。

最近では、システムの機能停止や情報漏洩等の情報システムをめぐる事故や事件が起こるたびに、その原因が技術上・管理上の問題にあったとしても、それを未然に防げなかった経営責任が問われ、「ガバナンス不在」と言われることが多くなってきている。

情報システムは企業内の事業や業務活動にとって不可欠なものとなっているだけでなく、ネットワークを通じてさまざまなステークホルダーとの繋がりを持つようになってきている。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のである。その意味で、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。

２.コーポレート・ガバナンス、IT ガバナンス、IT 管理の関係

次ページの図１に示すように、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。

一方、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。

このように IT ガバナンスは、情報システム部門の管理者や専門技術者が対処すべき技術的な管理、あるいは情報システムのユーザ部門や業務部門の管理者が日常的に行う運用管理としての「IT 管理」とは明確に区別されるものである。

IT ガバナンスといっても、特別なガバナンスの仕組みがとられたり、監査役による特別な監査が必要となるわけではない（Q１参照)。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]。

事業活動や業務活動のなかでの IT 利活用の重要性が高まれば高まるほど、コーポレート・ガバナンスの一側面としての IT ガバナンスの比重も高まってくる関係にある。

今日のように、経営戦略はもとより、業務活動にも幅広く IT が利活用されている企業環境にあっては、効果的なコーポレート・ガバナンスの実現にとって、IT から目を背けることはできず、その意味で、「IT ガバナンス」の重要性が高まってきているのである。

また、今日、管理者層によって行われるさまざまな管理活動も、IT の利活用を抜きにしては考えられなくなってきており、「IT 管理」も情報システム部門だけに依存した特殊な管理ではなくなってきている。その意味でも、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のである。

---

[1] リスクをもって、「事象や意思決定に伴って生じ得る将来の帰結のブレ」と広く定義すれば、企業活動に伴って生ずるリスクは、企業価値の向上に結びつく「アップサイドリスク」と、企業価値の毀損に結びつく「ダウンサイドリスク」からなる。監査役監査の基本的立場からすれば、第一義的には、情報システムの機能停止や不正利用等による損失発生のリスクや損害賠償のリスク、さらにはレピュテーションの毀損に結びつくダウンサイドリスクに着目すべきである。しかしながら、IT の利活用には、新たな事業開拓や競争優位性の確保、さらには業務活動の効率化といった側面もあるから、そのようなアップサイドをどのように向上させるかという視点からするガバナンス機能の発揮も必要であろう。

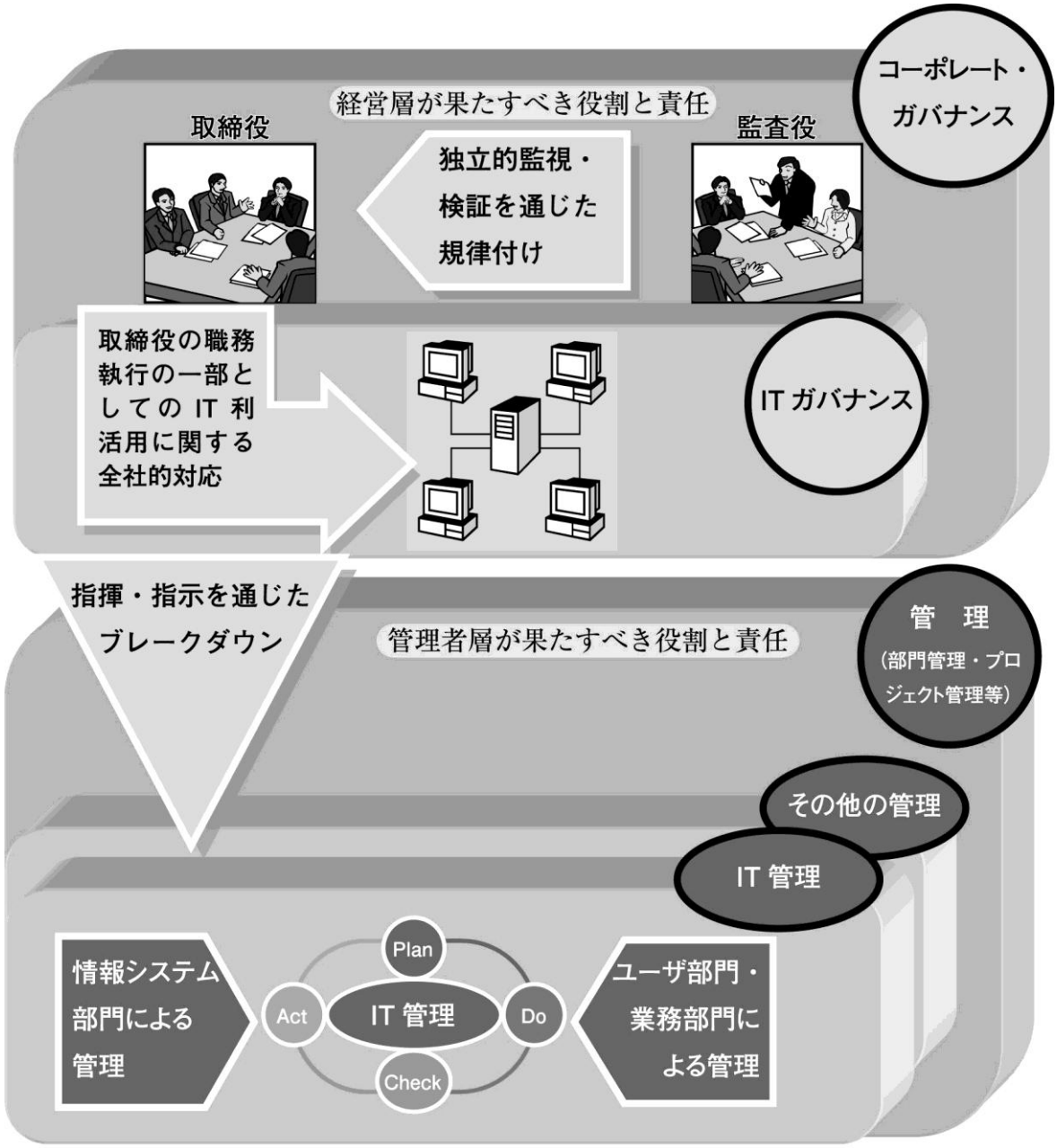


図１　ガバナンスと管理（マネジメント）の関係

３.IT ガバナンスの重要性と監査役としての関わり方

「ガバナンス」をもって企業組織としての全体的な方向付け、及びそれをリードすべき取締役に対する規律付けとみれば、取締役が果たすべき役割・責任と、監査役が果たすべき役割・責任は、まさに「車の両輪」である。

今日のように、情報システムの利活用抜きに事業活動・業務活動の遂行が考えられない環境においては、情報システムの機能停止や誤動作が大幅減益、顧客喪失、信用失墜にも繋がりかねず、また機密情報や顧客情報の漏洩など情報システムを悪用した不正行為によって莫大な損失を被るリスクも常に想定しておく必要がある。個人情報の漏洩等が企業内部犯であるような場合には、会社としての法令遵守体制が問われることにもなりかねない。

しかしながら、このような IT リスクは、文字通り、情報システム部門や、開発・運用の委託先（ベンダー）が「技術的に」管理すべきものと考えられがちで、ユーザ部門や取締役が管理し対処すべきリスクとは見られない傾向がある。情報システム部門やベンダーへの押し付け、丸投げとなりやすいのである。

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。

また、事業戦略の立案には、IT をどのように利活用するかという視点が欠かせなくなってきていることも多い。「IT 戦略」というのは、単に、情報システムの技術戦略ではなく、企業の事業戦略と融合されている必要がある。情報システムそれ自体が目的とはなり得ないからである。その意味で、監査役は、IT への投資の失敗が招くリスクや、事業戦略を効果的に達成できないリスクという観点から、取締役の職務執行を監視・検証する必要がある。

さらには、業務活動レベルにおいても IT 利活用の成否が業務の有効性と効率性を大きく左右するようになっており、かつ、今日のように情報システムが企業の経営活動に深く浸透している状況においては、情報システムの機能停止が事業活動・業務活動の停止に直結する事態も想定しておかなければならない。これらのリスクは、事業活動・業務活動への情報システムの浸透度合いが高ければ高いほど企業経営に与える影響が大きくなってくるという前提で、監査役は、取締役が経営リスクとして適切な対応を行っているかどうかの監視・検証を通じてガバナンス機能を発揮すべきである。

このように、IT の利活用に伴って生ずる IT リスクは、その原因が技術的な要因であったり、現場で対応すべきレベルの事項であったとしても、取締役の対応が必要となる経営リスクにつながる可能性が高い。

その意味で、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のである（図２を参照）。

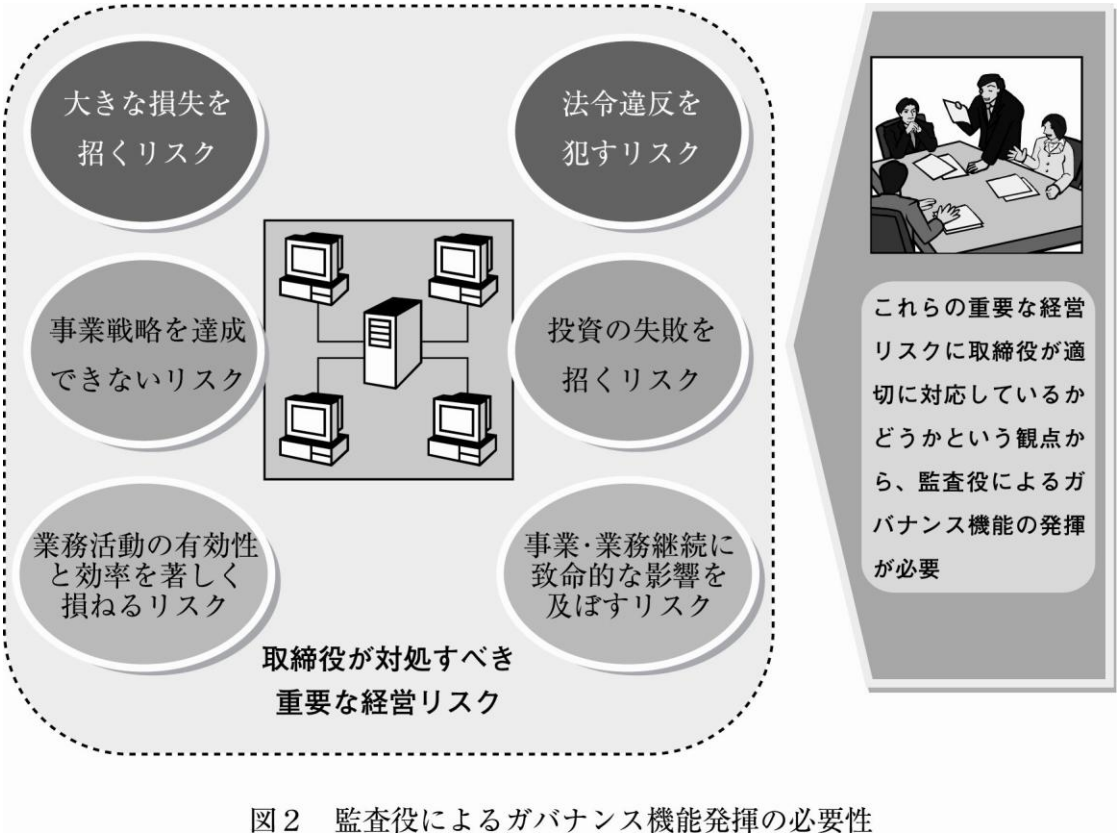


図２　監査役によるガバナンス機能発揮の必要性

＜参　考＞　IT リスクの原因事象の例

[システム的原因又はシステムの脆弱性に関係するものの例]

- システムへの不正侵入
- コンピュータ・ウィルスの感染
- プログラムのバグ（誤り）
- システムへの加重負荷
- 回線障害
- ホームページの乗っ取り

[人的・組織的原因に関係するものの例]

- 入力ミス
- データの不当な書き換え
- データ/情報の漏洩
- データの消失
- PC/携帯端末/外部記憶媒体の盗難/置き忘れ
- メールの誤送信

Q１：IT ガバナンスへの取組み方の要点は？

Q これまで IT に関係する業務を経験したこともなく、IT と聞いただけで引いてしまいます。このような場合でも IT ガバナンスの機能を発揮することは可能でしょうか。もし可能ならば、どのように IT ガバナンスに取り組めばよいでしょうか？

A 監査役は、IT ガバナンスをもって特別な概念として捉える必要はまったくありません。コーポレート・ガバナンス機能の発揮の一環として、取締役が果たすべき IT を利活用した情報システムに関する職能と責任を、独立の立場から監視・検証すること、そのものなのです。

「監査役監査基準」を見てみましても、第 40 条で文書・情報管理の監査、第 41 条で法定開示情報等に関する監査、第 56 条で電磁的方法による開示等が規定され、これらは IT が前提となっています。また、「内部統制システムに係る監査の実施基準」でも、第 10 条で情報保存管理体制に関する監査が規定されています。しかしながら、IT に関する専門知識は必ずしも必要ではなく、各基準に定められた手順等に基づき監査を実施すればよいのです。

IT が組み込まれた業務の性質や重要性に応じて、取締役が IT 利活用に係るリスクを認識しているかどうか、そのリスクの影響を部門横断的に把握できる仕組みを設けているかどうか、情報システムの長時間にわたる機能停止などの緊急事態にも対応できる体制をとっているかどうか、さらには巨額の IT 投資などではその失敗が致命傷になりかねないので、開発・導入体制に重大な欠陥がないかどうかなどを、取締役の職務執行の監査という目線でチェックすればよいのです。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となり、IT ガバナンスの機能を担うことになるのです。

４.監査役から見たITガバナンスとはどのようなものか

（１）ITガバナンスとは何か

IT ガバナンスの定義については、これまで幾つかのものが示されてきたが、コーポレート・ガバナンスとの関係を意識しつつ、かつ監査役の職能と責任を明確に反映して定義すれば、次のようになる[2]。

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。

＜参　考＞　IT ガバナンスに関する代表的な定義

- 経済産業省「企業が、IT に関する企画・導入・運営及び活用を行うにあたって、すべての活動、成果及び関係者を適正に統制し、目指すべき姿へと導くための仕組みを組織に組み込むこと、又は組み込まれた状態。」
- IT ガバナンス協会「IT ガバナンスは、企業のガバナンス全体の不可欠な構成要素であり、組織の IT が組織の戦略ならびに目標を維持し発展させることを保証するリーダーシップと組織構造、さらにプロセスから構成されている。」
- ISO/IEC38500「現在及び将来の IT を指揮し、管理するシステムであって、企業の IT ガバナンスには、組織を支援する IT の活用を評価し、指揮すること、及び計画を実現するためにこの活用を監視することが必要となる。これには、組織内で IT を活用するための戦略及び方針が含まれる。」

コーポレート・ガバナンスは、経済学、法学、経営学などの領域ごとにさまざまな意味で用いられているが、株主の利益保護や取締役に対する規律付けだけでなく、さまざまなステークホルダーを意識した企業価値の向上や企業の社会的責任の履行という対外的な視点も含めて、幅広く企業経営の仕組みなりあり方を意味するようになってきて

[2] ちなみに、2001 年、当協会内に設置された IT ガバナンス委員会報告では、IT ガバナンスをもって次のように定義していた。「IT ガバナンスとは、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、さらに、このリスクとパフォーマンスのマネジメント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。」この定義は、経営効率の最大化を前面に出し、健全性の確保を併記していることからも分かるように、「経営への IT の戦略的利活用」という視点に重点を置いたものであった。（『月刊監査役』448 号、2001 年 9 月号所収「IT ガバナンスにおける監査役の役割」）

いる[3]。

そのような企業経営の仕組みとしてのコーポレート・ガバナンスを形式的な仕組みとしないためには、上記の対外的な視点を達成するための前提として、企業としての事業継続と組織内の業務の有効性及び効率性を図るという対内的な視点も含めて考えておかなければならない。

IT ガバナンスは、コーポレート・ガバナンスのうち IT の利活用に関するガバナンス機能をいう。今日の企業活動の多くが IT の利活用なくしては成り立たなくなってきている。IT の利活用が進んだ経営環境では、大局的な観点からする取締役の対応と、監査役によるその監視・検証が不可欠となってきており、コーポレート・ガバナンスのなかでも、IT ガバナンスに着目することが重要となってきているのである[4]。

Q２：IT ガバナンスと ERM の違いは？

Q 「ERM（Enterprise Risk Management)」という用語を耳にしますが、IT ガバナンスとはどのように違うものなのでしょうか？

A 内部統制という概念の拡張として ERM の重要性が広く認識されるようになりました。その考え方を要約すれば、①リスク管理への取組みをグループ全体で統一的に行うこと、②関連するリスクを横串で管理すること、③損失だけでなく利得にも帰結し得るリスクも管理の対象とすること、といった点に集約できそうです。このように、ERM は、全社挙げての、経営リスクへの統合的な取組みといってよいでしょう。

ERM は、経営者主導による全社的なリスク対応に焦点がありますので、その点で IT ガバナンスと共通点を持ちますが、その一方で監査役の果たすべき役割や責任に曖昧さが残ります。しかし、IT ガバナンスには、全社的なリスク対応という意味の他に、経営者（取締役）に対する規律付けという意味がありますので、監査役の立ち位置が明確になります。

したがって、ERM を導入することと、IT ガバナンスを確立することは同じことではありません。

---

[3] この点について、神田秀樹氏はつぎのように指摘している。「コーポレート・ガバナンス（企業統治）とは、どのような形で企業経営を監視する仕組みを設けるかという問題であるが、不正行為の防止（健全性）の観点だけでなく、近時は企業の収益性・競争力の向上（効率性）の観点からも、コーポレート・ガバナンスのあり方について世界的な規模でさまざまな議論がなされている。コーポレート・ガバナンスは、会社法などの法制だけにかかわる問題ではなく、実際上の対応も重要である。」（神田秀樹『会社法（第９版)』弘文堂、2007 年、150 頁。）

[4] IT ガバナンスをコーポレート・ガバナンスと密接に結びつけて理解する考え方は国際的な流れでもあり、たとえば ISACA を母体とする IT ガバナンス協会は、IT ガバナンスをもって取締役会ならびに役員の責務であるとし、企業のガバナンス全体の不可欠な構成要素であるとしている。（IT Governance Institute, Board Briefing on IT Governance, 2nd ed.,2003, p.10.　ISACA 東京支部・日本 IT ガバナンス協会訳「取締役会のための IT ガバナンスの手引」、12 頁。）

Q３：IT ガバナンスのためのチェックリストは？

Q　当社では、事業活動や業務活動の遂行にとってもはや情報システムはなくてはならないものとなっています。そこでこれから IT ガバナンスにも前向きに取り組みたいのですが、その際に活用できる監査役のための「チェックリスト」のようなものがあるとありがたいのですが、何か適当なものはありませんか？

A　監査役としての IT ガバナンスへの取組みは始まったばかりですので、残念ながら「これ」といった決定的なものはありません。また、本文でも述べていますように、IT ガバナンスは監査役の任務そのものでもありますから、チェックリストに従って、一つひとつ潰してゆくことが IT ガバナンスではありません。

ただ、そうは言っても、なかなか取り組み難いのが現実でしょうから、本報告書では、＜付録、47 頁＞として、会社法施行規則に基づいて構築が義務づけられている内部統制システムに則して、IT の利活用環境に落とし込んだ場合の監査上の着眼点を一覧で整理しておきましたので、まずはそれを参考にしながら取りかかられるとよいと思います。

また、IT ガバナンス協会という国際組織が『取締役会のための IT ガバナンスの手引』と題するレポートを公表しています（情報システムコントロール協会東京支部のホームページ http://www.isaca.gr.jp から翻訳版が入手可能です）。このレポートは「企業価値向上」という視点を強く打ち出した内容となっている点に特徴があります。バランススコアカードを応用した考え方なども紹介されていますので、アップサイドリスクへの対応という観点から取組みを行おうとされる場合には一度ご覧になっておかれるとよいかもしれません。

当該レポートの付録には、たとえば「取締役会は、ビジネス要因の視点（顧客へのサービス、コスト、迅速さ、品質）からする IT の価値を示す IT 成果報告書を受け取っているか」といったチェック項目をはじめ、47 の項目が示されており、それぞれの項目が「価値の提供」「戦略との整合性」「資源の管理」「リスクの管理」「成果の測定」という IT ガバナンスの重点領域とマトリクス形式で対応付けられています。

（２）IT ガバナンスが目指すもの

コーポレート・ガバナンスとの関係を意識しながら、IT ガバナンスの目的を挙げれば、図３のようになる。

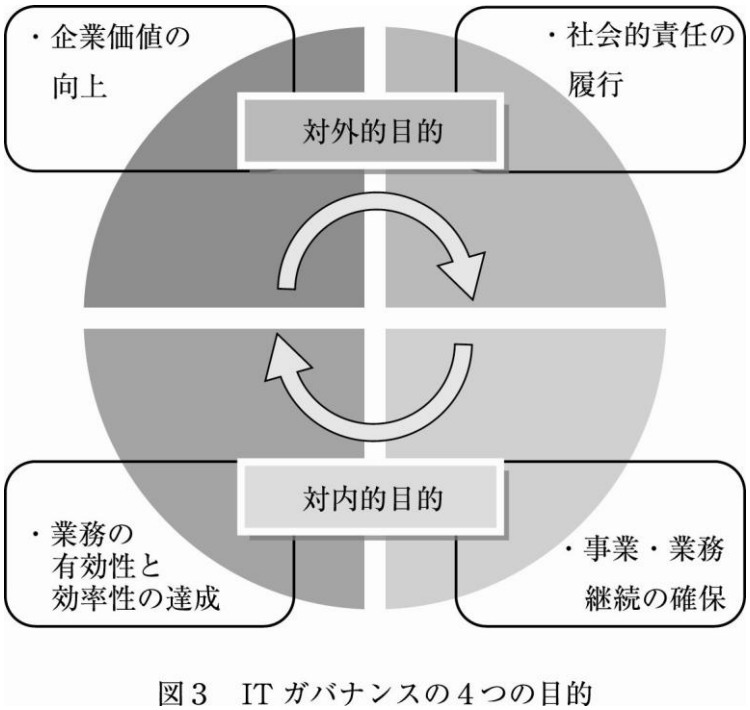


図３　IT ガバナンスの４つの目的

図３に示したように、「企業価値の向上」及び「社会的責任の履行」という目的は、企業外部のステークホルダーを意識した対外的・外向きの意味をもつ目的である。

＜企業価値の向上＞

IT に支えられた今日の経営環境において、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ことは改めて述べるまでもないであろう。また逆の言い方をすれば、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。

株価への影響に限定しても、情報セキュリティをめぐるリスクが顕在化したとき株価は下落すること、リスクが顕在化したときにそれを隠蔽したり追加の事故が発覚すると株価は長期にわたって回復できないこと、リスク情報をあらかじめ開示していた企業の方がそうでない企業に比べて株価回復が早いことは、実証研究によっても確かめられている[5]。

また、ある大手事務機器メーカでは、情報セキュリティを通じた組織ブランドの向上を謳い、「法令規制対応」（外部要因への対応に迫られて個別に取組むレベル）、「情報セキュリティマネジメント」（企業市民としての使命感から会社全体で取組むレベル）を経て、「情報セキュリティ経営」（情報セキュリティ活動を通じて利益創出を図るレベル）

[5] 経済産業省・情報セキュリティ政策室編『情報セキュリティガバナンス』（財）経済産業調査会、2009 年、15―16 頁参照。

を目指すとしている。

＜社会的責任の履行＞

企業の社会的責任の履行という目的では、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[6]。なかでも情報開示は、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。

一方、「事業・業務継続の確保」及び「業務の有効性と効率性の達成」という目的は、対外的目的を実現するための組織としての取組みという企業の対内的・内向きの意味をもつ目的である。

＜事業・業務継続の確保＞

情報システムはそれが事業・業務活動に深く浸透すればするほど、ごくわずかなシステム停止がさまざまな影響を及ぼす可能性がある。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。

とりわけ東日本大震災を契機として事業・業務継続の確保が注目されるようになり、サプライチェーンを支えている情報システムをいかに保護するかは喫緊の課題ともなっている。

＜業務の有効性と効率性の達成＞

情報システムは社内業務の有効性と効率性を達成する上で不可欠なものである。情報システムを導入したものの、それが業務改善に結び付かなかったというケースは少なくない。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。効率も同様であり、情報システムの処理性能が向上しても、それは業務の効率向上に結び付いていなければならない。

いうまでもなく、上記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。

すなわち、企業価値の向上は企業の社会的責任の履行を無視しては成り立たず、これら外部目的の達成にとって、企業の事業・業務を安定的に継続し、かつ業務の有効性と効率性を達成することは不可欠な要件となる。また、対内的目的である事業・業務継続の確保と業務の有効性と効率性の達成は、結果として企業価値の向上にも結びつくとい

[6] ISO26000:2010、“Guidance on social responsibility”（社会的責任に関する手引）では、「社会的責任の原則」として、「説明責任」、「透明性」、「倫理的な行動」、「ステークホルダーの利害の尊重」、「法の支配の尊重」、「国際行動規範の尊重」、「人権の尊重」からなる７つを挙げている。なお、訳語は(財)日本規格協会のものによる。

うように、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のである。

Q４：リスクへの対応と企業価値向上の関係は？

Q　これまでの IT ガバナンスについての議論を仄聞する限り、情報システムの機能停止や情報漏洩などのように会社に損害を及ぼすリスクよりも、むしろ IT の戦略的な利活用を通じた企業価値向上に焦点が当てられているように思えてなりません。そうなると、監査役はどこまで踏み込むべきか、また踏み込めるのか疑問です。

A　「ガバナンス」という用語が企業価値向上といった言葉と結びつけられて使われることも多くなり、その影響もあってか IT ガバナンスには、IT を事業戦略にいかに生かすかとか、IT 投資をいかに効果的に行うかといった戦略的な側面が強調されることがあります。ご質問の趣旨は、IT ガバナンスをもって、取締役の職能として限定的に見たときの理解といってよいでしょう。このような事業戦略や投資戦略の立案と実行そのものは、取締役の経営意思決定そのものであり、取締役の専管事項ですから、監査役がそれに直接関与することはあり得ません。

IT 戦略や IT 投資の失敗が会社に重大な損害を及ぼす可能性は払拭できません。監査役は取締役の職務執行を監査することでガバナンスの機能を発揮するわけですから、取締役がかかるリスクを十分に認識し、取締役会で議論された上で決定がなされているかどうかを監視し検証する必要があります。IT ガバナンスは、取締役の役割と責任にくわえ、監査役による独立的監視・検証を通じた規律付けがあって、はじめて有効に機能するものです。経営意思決定に伴うリスクというのは、常に利得と損失が表裏一体のものとなっているという前提で、監査役は取締役の意思決定に目を光らせるべきです。

もし取締役が、IT の戦略的利活用による効果や利益の創出をいかに極大化するか、それを阻害するものは何かという見方しかしていなければ、監査役は当該意思決定に伴って生ずるであろう直接的・間接的な損失発生のリスクに十分な注意を払う必要があります。

IT の戦略的な利活用がいかに重要であっても、個人情報漏洩対策などに手落ちがあっては、会社としての法令遵守体制が疑われてしまいます。そこで監査役は、まずもって情報システムの機能停止や情報漏洩など、IT の利活用に伴う損失発生のリスク、とりわけ法令遵守体制に対する取締役の対応が必要かつ十分なものであるかどうかに着目し、その上で IT の戦略的な利活用の失敗に伴うリスクにも目を向けることで取締役の注意を喚起するという姿勢が現実的でしょう。そうすれば、取締役の経営判断の妥当性にまで踏み込むことなく、監査役としてのガバナンス機能を果たすことができます。

（３）IT ガバナンスを構成する要素とは

コーポレート・ガバナンスとの関係を意識しながら、IT ガバナンスの構成要素を挙げれば、図４のようになる。

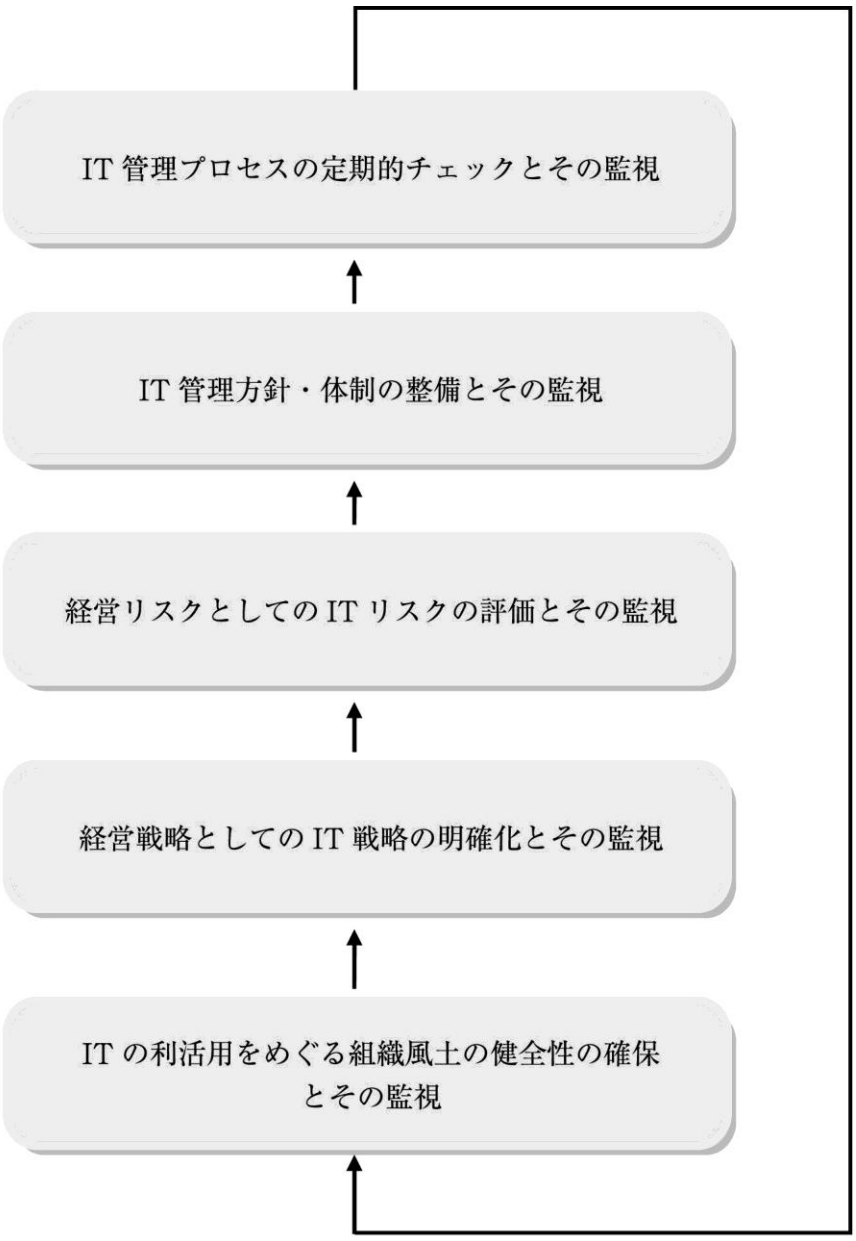


図４　IT ガバナンスの５つの構成要素

＊　上記の構成要素に含まれる「監視」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」からなっている。

IT ガバナンスは、「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」が土台となっている。情報システムがさまざまな業務に広く活用されている状況においては、情報システムの利便性だけでなく、その利用に伴うリスクが組織構成員に正しく理解され、全員でセキュリティ対策を遵守しようとする風土が醸成されていなければならない。取締役がいかに立派な IT 戦略を立案し、リスク評価に基づくしっかりとしたセキュリティ対策を構築しても、システムや業務を実際に動かすのが「人」である以上、組織構成員がリスクに敏感になり、コンプライアンス意識をもって業務に当たり、問題を引き起こす可能性のある事象や情報が共有されるとともに、適時に取締役に報告されるような健全な組織風土がすべての土台となるのである。

その土台の上に、「経営戦略としての IT 戦略の明確化とその監視」を前提として、「経営リスクとしての IT リスクの評価とその監視」が行われる。IT リスクの評価は、IT 戦略に基づいて行われるべきものであるから、IT リスクの評価とその監視は、IT 戦略の明確化とその監視の上に成り立っている。IT 戦略に基づいてリスク評価を行うことで、IT リスクは「技術のリスク」、「現場で対処すればよいリスク」ではなく、取締役と監査役が対処すべき「経営リスク」として認識されることになる。

ついで、全社的あるいは企業グループとしての「IT 管理方針・体制の整備とその監視」、及びそれを受けて全社的あるいは企業グループとしての「IT 管理プロセスの定期的チェックとその監視」が行われるが、それらは IT 戦略と IT リスクの評価結果に基づくものでなければならない。

取締役は、文書化された IT 管理方針や、各業務部門から上がってきた IT 管理についての要約レポートだけに目が向きやすい。それだけに監査役は、IT 管理の方針や IT 管理のプロセスが、IT 戦略と IT リスクの評価結果に基づくものとなっているかどうかという視点を忘れてはならない。とりわけ、IT リスクの評価結果については、たとえば「システムへの不正侵入のリスクの発生可能性と重要性」といった個別的・技術的な視点ではなく、「そのリスクが事業経営にいかなる影響を及ぼす可能性があるか」という経営リスク評価の視点で見る必要がある。そうでないと、形式的な監視・検証に終わってしまうか、取締役が行うべきリスク判断の適否を見誤ってしまうことになる。

このように、５つの構成要素は、それぞれがバラバラに機能するものでなく、体系性をもった「一連のチェーン」として理解されるべきものである。

さらに、重要な点は、これらの構成要素が連鎖的・有機的に結びついて機能することで、フィードバックが生まれ、より強固な土台の構築、すなわち「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」が可能となるという関係にあることである。

（４）IT ガバナンスの全体像（フレームワーク）

図５は、すでに述べてきたIT管理との関係、ITガバナンスの構成要素を組み込んで、IT ガバナンスの全体像（フレームワーク）を図解したものである。

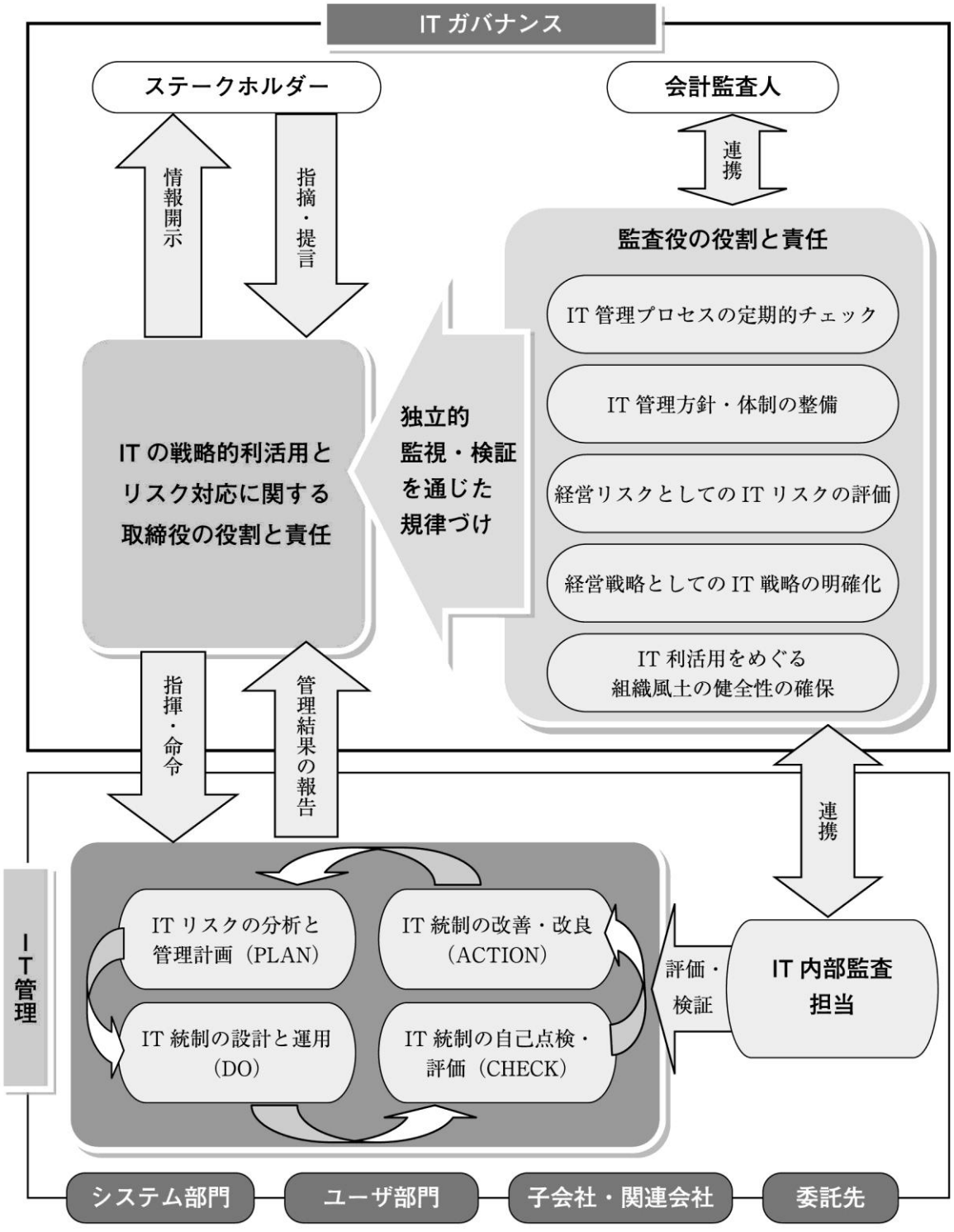


図５　IT 管理との関係を踏まえた IT ガバナンスの全体像

IT ガバナンスは、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」と、その独立的監視・検証を担う「監査役の役割と責任」が車の両輪となって機能する。図５の「監査役の役割と責任」というボックスの中に示された５つの基本的な役割は、すでに図４で示した「IT ガバナンスの構成要素」に対応している。

このように、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。

以下では、図５の「矢印」部分に着目して、IT ガバナンスの５つの基本的な構成要素が、その他の IT ガバナンスの構成要素（ステークホルダー及び会計監査人）や IT 管理（管理機能と IT 内部監査担当）と、どのような連携又は関係にあるかについての追加的な説明をしておきたい。

＜ステークホルダーとの関係＞

ガバナンスという概念は、そもそも企業外部のステークホルダーとの関係をも意識したものであるから、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、法定開示・適時開示書類（有価証券報告書、決算短信、コーポレート・ガバナンス報告書など）だけでなく、さまざまな媒体を通じて、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といえよう。

＜会計監査人との連携＞

一方、法令上、監査役には会計監査人の監査の方法と結果の相当性判断が求められていることから、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。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。

＜IT 管理との関係＞

IT 管理（マネジメント）は、「IT リスクの分析と管理計画（PLAN）」、「IT 統制の設計と運用（DO）」、「IT 統制の自己点検・評価（CHECK）」、「IT 統制の改善・改良（ACTION）」を構成要素とする PDCA サイクルからなり、部門管理者層が担う個別具体的な管理活動である。

図５に示した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。このように、IT

ガバナンスは IT 管理と密接に関連づけられることで機能する。

＜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。IT 管理の内部監査は、IT についての専門知識をもった IT 内部監査担当者によって通常の業務監査とは別に実施されている場合もあるし、業務監査の一環として実施されている場合もある。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。

ここで注意しなければならないことは、IT 管理は、システム部門の管理者だけに任せるのではなく、できる限りユーザ部門の管理者によっても行われなければならないことである。また、企業グループとしての IT 管理体制構築のためには子会社・関連会社の管理が必要となるし、情報システムの開発や運用がベンダーに委託されている場合には委託先の管理もカバーしておかなければならない。

＜参考：有価証券報告書におけるステークホルダーへの IT リスク情報開示の実例＞

1-A 情報漏洩リスクに関する開示例	当社グループは、「個人情報を個人情報保護法の定めに従い取り扱わなければなりませんが、」当社グループが、「かかる情報を保護できなかった場合、これにより生じた経済的損失または精神的苦痛に対し、賠償しなければならない場合があります。また、情報保護対策を実施するために、多額の費用が発生し、または通常業務に支障が生じる可能性があります。加えて、情報漏えい事故が発生した場合には、」当社グループの「業務、システムまたはブランドに対する社会的信用が低下し、」当社グループに対する「顧客および市場からの信頼を失い、」当社グループの「事業、業績および財政状態に重大な悪影響を与える可能性があります。」
1-B 情報漏洩リスクへの対応に関する開示例	「当社は個人情報の取扱いに関する重要性、危険性を十分に認識し、個人情報の適切な管理を実現するために、個人情報保護規程を整備しております。さらに、当社のホームページに個人情報保護方針を公開し、これら規程及び方針に準拠した行動指針やガイドラインを制定するとともに、役職員への教育、研修を通じて、個人情報を適正に管理する体制の構築に注力しております。なお、当社は、平成 13 年 7 月にプライバシーマーク制度（企業の個人情

	報保護体制が JIS Q 15001 に準拠しているか否かを財団法人日本情報処理開発協会（JIPDEC）が認証する制度）の認証を受けております。しかしながら、個人情報の収集や管理の過程等において、不測の事態により個人情報の漏洩等が発生した場合、当社への多額の損害賠償請求やプライバシーマークの認証取消処分または罰金等が課されるなど、当社の事業及び業績に影響を与える可能性があります。」
2-A システム障害リスクに関する開示例	「停電、災害、ソフトウエアや機器の欠陥、コンピュータウイルスの感染、不正アクセス等予測の範囲を超えた出来事により、情報システムの崩壊、停止または一時的な混乱、顧客情報を含めた内部情報の消失、漏洩、改ざん等のリスクがあります。このような事態が発生した場合、営業活動に支障をきたし、当社グループの業績に影響を及ぼす可能性があります。」
2-B システム障害リスクへの対応に関する開示例	「当社では、情報セキュリティマネジメントシステムを整備しており、当社ホームページに情報セキュリティ基本方針を公開し、当該方針に準拠した行動指針やガイドラインを制定すると共に、教育、研修を通じて、適切な情報セキュリティの実現をはかっております。なお、当社は情報セキュリティマネジメントシステムに関する国際規格である ISO/IEC27001:2005/JISQ27001:2006（平成 17 年 3 月に取得した BS7799-2 及び ISMS 認証基準 Ver.2.0 より平成 19 年 1 月に移行取得）の認証を受けております。しかしながら、当社の予測を超える当サービスのシステムへの不正アクセス、盗難、紛失等により、または情報セキュリティ対策の不備により、情報資産の漏洩、紛失、改竄等があった場合、当社への多額の損害賠償請求や認証資格の取消処分または罰金等が課される可能性があり、当社の事業及び業績に影響を与える可能性があります。」
3-A 重大な災害リスクに関する開示例	「地震、火災、洪水等の災害(気候変動の進行によって発生するものも含む)や戦争、テロ行為、コンピューターウイルスによる攻撃等が起こった場合やそれにより情報システムおよび通信ネットワークの停止または誤動作などが発生した場合に、当社グループの拠点の設備が大きな損害を被り、その一部の操業が中断し、生産・出荷が遅延する可能性および損害を被った設備の修復費用が発生する可能性があります。」

3-B 重大な災害リスクへの対応に関する開示例	当社グループでは、「国内の主要事業拠点の耐震化、防災訓練、情報システムの二重化等の事前対策を実施するとともに、緊急時の行動要領等をまとめた事業継続計画（BCP）を策定しています。しかし、これらの対策を実施しているにもかかわらず、」当社グループの「製品・サービスに対する需要が低下したり、」当社グループによる「製品の納入または仕入先による部品の納入が困難もしくは不可能となる可能性があります。さらに、損害を被った設備を修復または代替するために多額の費用が必要となったり、サプライチェーンにおいて遅れや効率性の低下を招く可能性もあります。」

＊　いずれも平成 22 年度版有価証券報告書から引用：なお、社名は伏せてある。

Q５：IT の専門技術や専門用語はどこまで理解すべきか？

Q　情報システム部門等へのヒアリングでは、専門用語やアルファベットの略語が入った資料を基に説明を受けますが、IT に関係する職場と無縁であった私には、とても理解できるとは思えません。情報システム部門には IT のベテランが揃っており、よく分からない者が口出ししてかえって現場の管理が混乱しないかという心配もないわけではありません。現場レベルで日々実践される技術的な IT 管理との関係で、技術的な部分についてはどこまで理解しておく必要があるでしょうか？

A　まずは、取締役が行うべき IT ガバナンスは、現場レベルで日々実践される技術的な IT 管理とは、別の異なったものと認識すべきでしょう。つまり、IT 管理レベルの日々の実務について、監査役が事細かな技術的な内容まで理解することは必須ではない、ということです。たとえば、IT 管理レベルの具体的内容として、障害管理が挙げられます。ソフトウェア、ハードウェアともに、日々色々な障害が発生します。その障害の原因や対応について、監査役は技術的に細かな点まで完全に理解できなくても大丈夫です。それよりもむしろ、監査役としては、これら障害の状況について、取締役に対して、事象発生時に、あるいは定期的に適切な報告が行われているか、それに対して取締役から的確な指示・命令が行われているかどうか、といった点を監視・検証し、もし行われていなければ、行うよう取締役に促すことがその役割といえます。ここまででお気付きのとおり、これら一連の業務の流れは、IT 以外の業務と同様です。したがって、IT の専門用語にいたずらに悩まされることなく、業務の大きな流れに留意してください。IT 管理の責任者等へのヒアリングでは、技術の仕組みを理解することよりも、管理の全体像に重要な問題点がないかどうかの確認こそが重要です。

第Ⅱ部
監査役としてのIT ガバナンスの取組み方

１．「IT ガバナンスの構成要素」ごとにみた取組みのポイント

（１）IT の利活用をめぐる組織風土の健全性の確保

すでに明らかにしたように、「IT の利活用をめぐる組織風土の健全性の確保」がすべての構成要素の土台である。この土台が揺らぐと、いくら堅牢な相互監視や独立的監視の仕組みを構築しても、企業価値向上はおろか遵法精神に欠けたりして企業の社会的責任を全うできない可能性が高まる。

しっかりとした IT 管理の仕組みを整えている企業であっても、個人情報漏洩、情報システムの誤操作・誤作動・機能停止などが絶えないのは、すべての企業構成員のモチベーションを高め、リスクに対する認識を根付かせるための組織風土に欠陥があるためであることが少なくない。実際に IT を動かし、管理するのもされるのも、意思と感情をもった生身の人間であり、組織はその集合体だからである。

その意味で、取締役は、企業目的の達成に向けた健全な組織風土や IT の利活用の環境を強力なリーダーシップのもとに構築しなければならず、監査役は独立的・客観的な立場からそのような取締役の姿勢を監視し、牽制する必要がある。

Q６：IT の利活用と組織風土の健全性確保の関係は？

Q IT の利活用をめぐる組織風土の健全性確保の重要性は頭では分かりますが、具体的にイメージできません。また、監査役がそれを確かめるためには具体的にどのようにすればよいのでしょうか？

A 良質なコーポレート・ガバナンスにとって想定されている組織風土と一体のものと考えてよいでしょう。経営理念及びコンプライアンス重視の経営姿勢が明示され、社員一人ひとりがルールを遵守し、迅速・適正な職務遂行を心掛ける健全な社内・グループ内環境のもとで、IT の利活用が行われているイメージです。

いくら厳格な管理を行っていても、それを運用するのは人間ですから、組織としてのモラールが低下していたり、ルーズな運用を容認するような職場環境であったりすれば、たちまち管理レベルは低下し、結果的に、経営にとってはかりしれないダメージを与える可能性があります。

全社的・グループ横断的な組織風土の状況を点検する一環として、IT の利活用に焦点を当てた場合、次のようなチェックポイントが考えられます。

- IT 業務に対し、会社はその重要性に見合う程度まで、人的・物的リソースを割いていますか。
- 社長など経営トップから IT の重要性に関するメッセージを発信していますか。
- IT 業務を担う部署に対する社内の評価は適正でしょうか。
- IT 部署の社員の士気は高く維持されているでしょうか。
- 情報子会社や外部業者（ベンダー）に任せっきりになっていませんか。

会社の組織風土の健全性確保のためには、IT 利活用による効果とそのリスクに対し、経営層はじめ、会社全体として認識を共有し、その共通認識のもとで業務が遂行されていることが重要です。

（２）IT 戦略の明確化

上記の健全な組織風土を土台として、IT を利活用した経営を方向付ける「経営戦略としての IT 戦略の明確化」が行われなければならない。長期的な経営ビジョンに基づく事業戦略と IT 戦略との整合性の確保、IT 戦略が内包するリスクの認識、戦略を実現するために必要な IT 投資に関する意思決定、さらにはそれらが適切に行われるための相互監視は取締役が担うべき役割である。

監査役は、取締役が行う経営判断の妥当性そのものを直接に監査の対象とすることはないが、IT の利活用方針を含む IT 戦略が不明確だと、全社的な方向付けができなかったり、IT 戦略を実現するための IT 管理の運用も曖昧なものとなり、結果として経営の根幹を揺さぶる問題に発展しかねない。そのため、監査役は、IT が経営戦略に組み込まれる場合、取締役会において十分な議論がなされているかどうか確認しておく必要がある。

Q７：IT 戦略の監査ポイントは？

Q　IT 戦略が明確になっているかどうかを監査する上でのポイントについて教えてください。

A　IT 戦略といいますと、どうしても IT 投資の妥当性にだけ着目しがちですが、中長期的な経営戦略のなかで IT 戦略がどのように位置づけられ、組み込まれているかという観点からの監視と検証が重要です（IT 投資の妥当性監査については Q14 を参照）。従来、手作業で行っていた社内業務を単に IT に置き換えるという発想ではなく、顧客サービスの向上などの対外的な視点が盛り込まれているかどうかが重要です。

経営戦略の中で IT の利活用が占める比重や重要性は企業によってまちまちですので、一般的な監査ポイントを挙げれば次のようになります。

- IT 戦略は、中長期的な経営ビジョンや事業計画の内容として又は一体的なものとして明確に定められているか。
- IT 戦略は、取締役会等で十分に議論されて決定されているか。
- IT 戦略は、わかりやすく社内に明示され周知が図られているか。
- IT 戦略は、情報システム部門やユーザ部門の業務計画に落とし込まれているか。
- IT 戦略は、達成状況が確認され、必要に応じ見直されているか。

今日では、IT 戦略の曖昧さは致命的な経営リスクに直結しますので、監査役としては、IT 戦略の妥当性そのものよりも、その失敗がどのような経営リスクに直結するかという視点をもつことが大切です。

（3）経営リスクとしてのIT リスクの評価

IT 戦略に基づいて全社的あるいは企業グループとしてのIT 管理方針が決定されるが、取締役の職務執行として重要なことは「経営リスクとしてのIT リスクの評価」である。これは、情報システムへの不正侵入リスクなどの個別具体的なIT リスクの「評価」（分析・測定）ではなく、取締役（あるいは取締役会）として対処すべき経営リスクとして認識することである。

IT リスクは他のリスクと同様、第一次的には業務の現場で対処すべきものではある。しかしながら、IT リスクは図６に示すように、現場での対処が必要なリスクに留まることなく、取締役が対処すべき経営リスク、すなわち事業継続リスク、顧客喪失リスク、損害賠償等の法的リスク、風評リスクなどへと連鎖・派生することが一般的である。

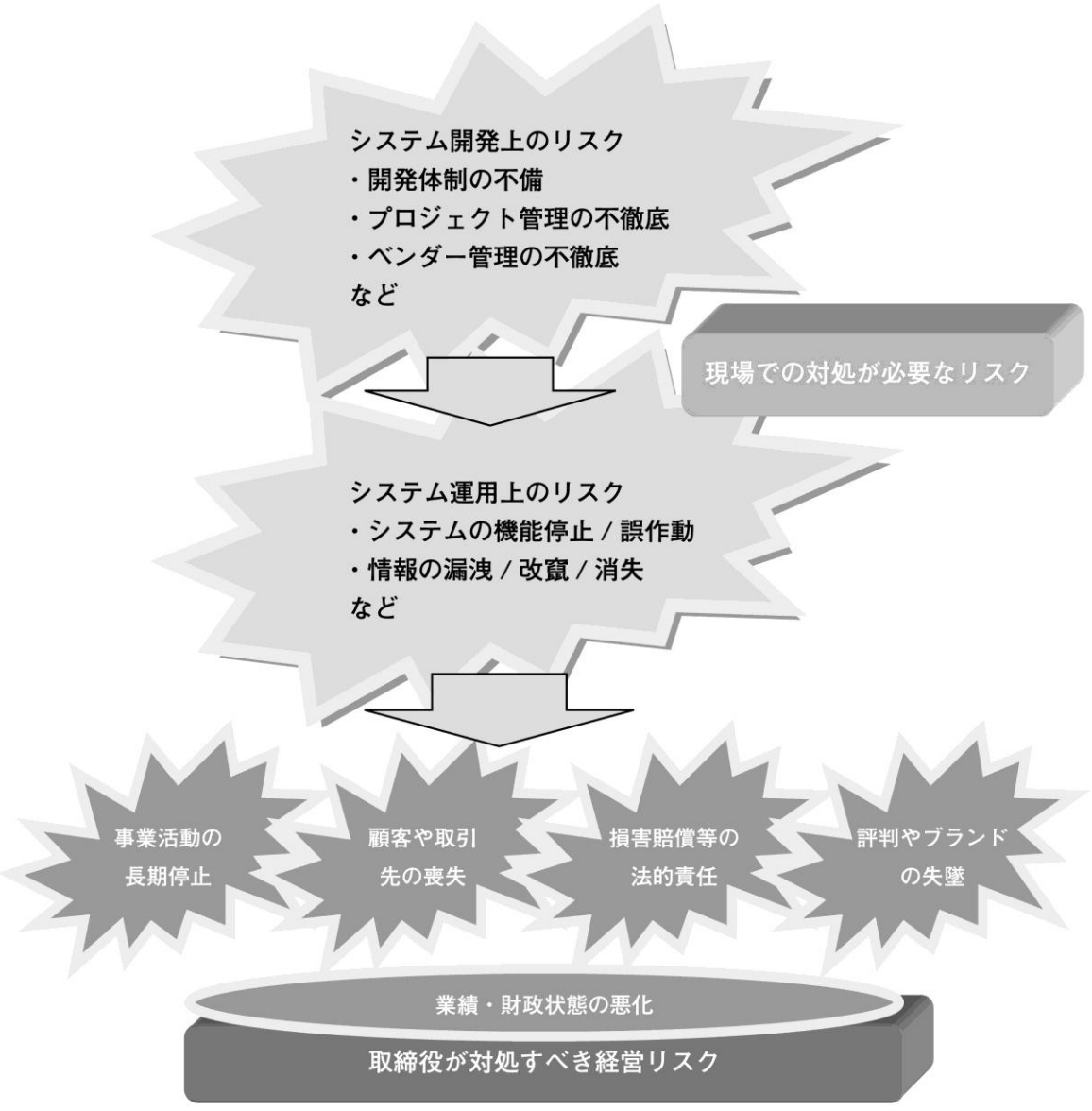


図６　IT リスクの連鎖・派生

したがって、IT リスクの認識は情報システムを所管する担当取締役だけでなく、すべての取締役が共有し、リスク認識とリスク対処についての相互監視が必要となる。

監査役は、IT リスクの連鎖・派生に注意を払い、それが取締役レベルで対処すべきリスクとなり得るかどうかを見極め、取締役の間でかかるリスク認識が共有されているかどうかを確かめておく必要がある。

Q８：システム開発の失敗リスクに対する監査ポイントは？

Q　IT リスクの中でもシステム開発の失敗リスクをどう回避するかが重要だと聞きますが、それはなぜですか。また、具体的にどのような点に留意して監査を行うべきでしょうか？

A　システム開発の失敗はその後のシステム運用や保守にも大きな影響を与え、かつ開発失敗リスクが顕在化したときには多額の損失を覚悟しなければならないからです。このようなシステム開発リスクには、システムの機能不足又は機能オーバー、予算超過、納期遅れなどがあります。なお、開発が外部委託されている場合の留意事項については、Q９を参照して下さい。

システム開発の失敗リスクを回避するための監査上の着眼点を挙げれば、次のようになります。

・開発プロジェクトのミッションが明確でプロジェクト関係者で共有されているか。
・開発の範囲及びレベルが明確か。
・開発コストの見積りは実績のある方法で、複数の手法で実施されているか。
・プロジェクト計画が作成され、承認されているか。
・プロジェクト計画をベースに進捗管理されているか。
・問題発生時にその内容と原因が経営層に正しく報告され、適切なアクションがとられているか。
・大規模基幹システムの開発状況については、定期的に取締役会等に報告されているか。

（４）IT 管理方針・体制の整備

取締役が経営リスクとして IT リスクを認識すると、それに基づいて「IT 管理方針・体制の整備」が決定され、部門管理としての IT 管理の実施へとブレークダウンされる。それは、取締役から管理者層への指揮・命令を通じて行われる。

Ｑ９：外部委託のリスクとその監査方法とは？

Q　当社では、情報システム部門を置かず、システムの開発・運用業務はすべて外部ベンダーに委託しています。したがって、組織上、情報システムの開発や運用についての取締役レベルでの責任が曖昧になりがちです。情報システムの管理体制の整備という観点から、このような状態は放置しておいてもよいものでしょうか？また、外部委託が行われている場合、監査役はどのような点に留意しなければなりませんか？

A　最近では、システム開発からその運用までをすべて外部に委託する企業も多いようですが、自社で行う場合に比べてコストが安くなる代わりに、委託先への丸投げ状態を放置するなど、さまざまなリスクを抱えます。したがって、外部委託を行う場合の窓口が明確になっているかどうか、担当の取締役が明確になっているかどうは監査役として確かめておく必要があります。

開発システムの重要性や投資規模に応じて異なりますが、大規模基幹システムの開発プロジェクトでは、取締役レベルのリーダーシップが必須です。プロジェクトメンバー全員にミッションステートメントを徹底させ、進捗をモニタリングし、ステアリングコミッティをリードしているかどうかを確かめる必要があります。

なお、外部委託の一般的な留意事項としては、①外部委託先選定方針・基準に基づき選んだ委託先で信頼がおけること、②契約において委託者としての権利を明確にしておくこと、③自社の責任体制を明確にしておくことなどが挙げられます。

①については、技術面はもちろんのこと、社内体制や財務状況が充実していることなどです。②については、委託者としての権利を明確に定めておくこと、たとえば再委託に対する同意、情報漏洩賠償責任、秘密保持義務、立ち入り監査等を織り込む必要があります。なお、契約書以外に、運用上のトラブルを避けるためには、委託先との間で、提供されるサービスの内容、範囲、品質に対する要求水準についてあらかじめ合意し、それを明文化した文書（SLA：Service Level Agreement）を取り交わしておく必要があります。③については、社内の責任体制として、実質的な発注部署（担当取締役）が責任を持つこととなりますが、経営に重大な影響がある外部委託案件については、全社的なリスク検討が必要でしょうし、取締役会等における監査役の適切な助言も必要となります。

（５）IT 管理プロセスの定期的チェック

部門管理者による IT 管理の結果は、定期的に取締役に報告されなければならず、それに基づいて「IT 管理プロセスの定期的チェック」が行われる必要がある。このとき、情報システム部門や IT の管理を所管する部門管理者からだけでなく、ユーザ部門管理者からも報告を受けていることを、監査役は確かめておくことが重要である。また、企業活動の根幹をなす情報システムの機能変更や運用体制の変更などは、新たな経営リスクを生むこととなることから、取締役会において十分な議論が必要となる。

Q10：技術レポートへの対応方法とは？

Q　当社の取締役会には、情報システム担当の取締役から、システムのパフォーマンスだとか、運用状況に関するきわめて細かな報告書が上がってきます。このような報告書へのコメントを求められた場合、どのように対応したらよいでしょうか？

A　まずもって注意すべきは、戦略なり、事業なり、業務にとってどのような意味をもっているかという観点からする分析レポートになっているかどうかということです。具体的には、第一に、システムの技術的なパフォーマンスの向上がそのまま業務活動の効率向上に必ずしも直結しているとは限らないということを理解しておくべきです。技術に明るい管理者ほどとかくシステムの細々とした点に深入りしがちです。しかし、システムの性能が向上しても結果として業務の有効性や効率性が高まらなければ意味がありません。取締役や監査役にはまずもってそのような目線が必要です。

第二に注意すべき点は、システム運用に関する業務上のボトルネックです。特にシステムに手が加えられたときには要注意で、「システム改修によって新たに生ずるリスクは何か」が明確に説明されていなければなりません。また、「システムの改修プロセスで何かトラブルや問題はなかったか」ということも確認しておく必要があります。

要は、たとえ技術的な内容のレポートであっても、常に「経営層として対応すべきリスクは何か」という目線でみて、それを裏付ける内容となっているかどうかを確かめることです。

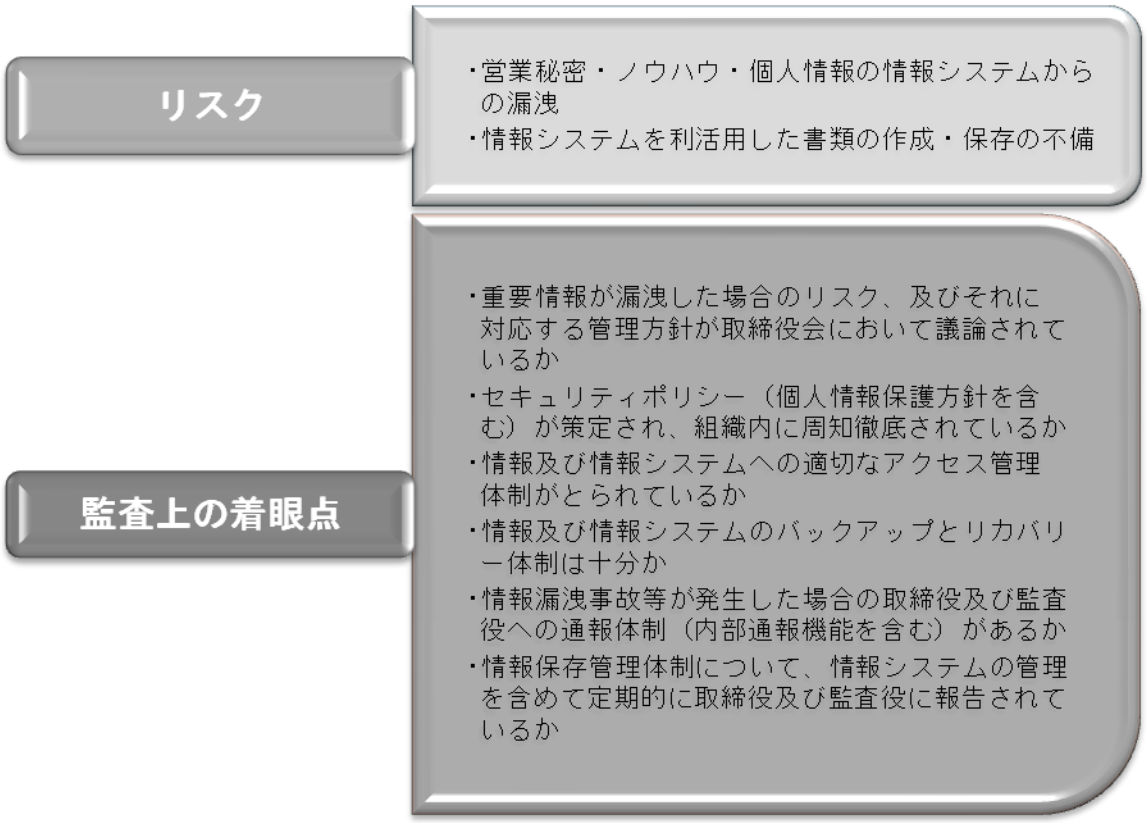
２．内部統制システム構築に即した取組みのポイント

（１）「会社法施行規則」に基づく取組みのポイント

①情報保存管理体制の監査

会社法施行規則第 100 条第１項で定められている内部統制に係る体制整備項目でも、最も IT との関係が深い項目である。したがって、IT の利活用という観点からは、内部統制システム構築の監査において、特に注意すべき項目である。

「内部統制システムに係る監査の実施基準」（第 10 条）では、IT の利活用を想定した「重要な営業機密、ノウハウ、機密情報や、個人情報のほか法令上保存・管理が要請される情報などが漏洩する結果、会社に著しい損害が生じるリスク」を例示し、それを受けて、「保存・管理すべき文書及び情報の重要性の区分に応じて、適切なアクセス権限・保存期間の設定、セキュリティー・ポリシー、バック・アップなどの管理体制が構築･運用されているか」という IT の利活用に関わる具体的な統制の要点を示している。



Q11：個人情報保護対策の監査事例は？

Q　当社は、顧客の個人情報を多数保有しており、もし当該情報が漏洩するようなことがあれば、会社の信用が大きく失墜する可能性があります。監査役監査では、どのような視点で個人情報保護対策を監視すればよいでしょうか？また、参考となる取組みを行っている事例があれば、教えてください。

A　①名刺ファイルの紛失、②メール・FAX の誤配信、③客先の氏名が入った携帯電話の紛失、④客先一覧の入ったノート PC の紛失、⑤個人情報の目的外利用などは、不注意から起こるケースがほとんどですが、社員が悪意をもって意図的に大量の個人情報を持ち出すとか、部外者がシステムに侵入してデータを盗み出すことも考えられますので、監査役としても、個人情報の管理体制が適切に整備され運用されているかどうかの監視と検証は重要になってきています。

管理方法は各社ごとにそれぞれあると思いますが、社内的な原因で情報漏洩が起こる場合がほとんどですので、まずもって社員の意識や認識を高めるための地道で定期的な教育研修が行われているかどうかを監視し検証することが、重要ではないでしょうか。

また、監査役監査としての取組み事例としては、次のようなものがあります。

【A 社の事例】当社では、以下の方法により監査を行っています。

① 各社員に配付されるコンプライアンス・ガイドブックに個人情報保護法が規定されていることを確認する。

② 個人情報保護を所管している CSR 委員会にオブザーバー出席し、また、下部組織である情報セキュリティ部会の事務局から当部会の審議状況をヒアリングする。

③ 事業場往査で現場の管理状況をヒアリングするとともに、内部監査部署から監査結果の報告を受ける。

【B 社の事例】当社では、平常時と事故発生時に分けた対応を行っており、それに従って監査を行っています。

平常時対応としては、プライバシーマーク制度で要求される JISQ15001 に従い、マネジメント・システムを導入していますので、①規程・ルールの整備（個人情報保護方針、個人情報保護規程、取扱いマニュアルの整備）、②教育計画の作成（最低年 1 回以上役職員に対して教育を実施）、③個人情報の取扱いの点検（部長が自部署で管理している個人情報を定期的にチェック）、④内部監査（内部監査室が定期的に全社の個人情報の取扱いを監査）、⑤経営者による見直し（事業年度末に経営者がマネジメント・システムの運用状況を評価・見直し）からなる一連の管理プロセスを大局的な観点から確認するようにしています。

また、事故発生時には、個人情報漏洩時に備えて独自に整備したマニュアルに基づき対応することになっていますので、その整備状況についても確認するようにしています。

Q12：情報漏洩対策のための監査の方法は？

Q　重要情報・機密情報は個人情報に限りません。重要情報・機密情報の管理が適切かどうかの監査を行うためには、情報システム部門長やユーザ部門長にどのような点を確かめておく必要があるでしょうか？

A　まずもって、重要情報・機密情報がもれなく把握され、重要度や機密度が情報ごとに識別されているとともに、重要度や機密度に応じた保護対策がとられているかどうかを確かめます。

次に、情報システム部門長やユーザ部門長に対して、以下の点についての説明を求め、とりわけ重要度や機密度が高い情報の保護対策については、当該対策の整備と運用状況についての資料の提出を求めます。やや技術的な事柄になりますが、重要情報・機密情報の漏洩は、会社に計り知れない損害を及ぼす可能性がありますので、監査役監査としてもその管理状況を確かめておけば安心でしょう

- ユーザ ID の管理状況：新規登録や、移動・退職等に伴う削除の手続きが明確に定められており、それが適切に運用されているかどうか。
- パスワードの管理状況：パスワードは定期的に変更することが義務づけられており、それが適切に運用されているかどうか。なお、通常のパスワードに代えて、使い捨て型パスワード（ワンタイム・パスワード）や指紋認証等の生体識別装置が使われていることもあります。
- アクセス権限の設定及び管理状況：重要度や機密度が高い情報へのアクセスに対しては、あらかじめ、きめ細かなアクセス権限（誰がアクセス権限を持つか、あるいは情報の閲覧は許可するが更新は制限するなど）が設定され、適切に運用されているかどうか。
- 暗号化の状況：重要度や機密度が高い情報（メールやファイル）は暗号化されているかどうか。
- PC ソフトウェアの管理状況：担当者の PC にファイル共有ソフト（ウィニーなど）が導入されていないことが定期的に確認されているかどうか。また、ウィルス対策ソフトが導入され、適時に更新されていることを管理者が確かめているかどうか。

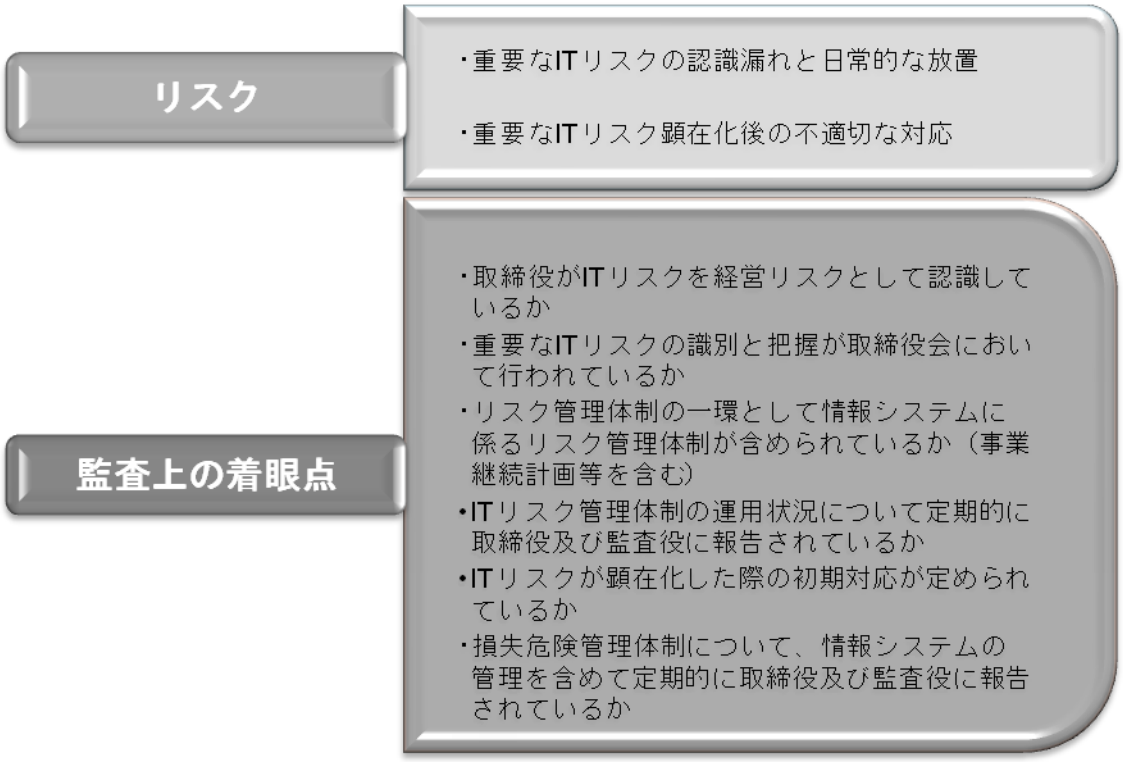
なお、東日本大震災を受けた節電対策の一環として在宅勤務が広がっており、PC の社外持ち出し、私用 PC による自宅からのアクセスを許可しているケースがあります。それに応じて、アクセス管理の変更や、セキュリティ・ポリシーの変更が必要となっていることもありますので、会社として適切なセキュリティ水準が確保されているかどうか確認しておく必要があります。

②損失危険管理体制の監査

IT リスクは、事業活動の長期停止、顧客や取引先の喪失、損害賠償責任の発生、評判やブランドの失墜など、企業の業績や財政状態にきわめて重要な影響を与える可能性がある。

「内部統制システムに係る監査の実施基準」（第９条）でも、IT の利活用と密接に関連するリスクとして「会社に著しい損害を及ぼすおそれのある事故その他の事象が現に発生した場合に、適切な対応体制が整備されていない結果、損害が拡大しあるいは事業が継続できなくなるリスク」を例示している。したがって、監査役は、IT リスクが経営リスクとなり得ることを取締役が十分に認識しており、リスク分析を踏まえた上で取締役会等において慎重な議論を行い、リスク対応計画とその定期的なレビューが行われているかどうかを監視し検証しなければならない。

なお、「実施基準」では、“各種リスク”に関する識別・分析・評価・対応のあり方を規定した管理規程が整備され、それに基づいた適切な運用とモニタリングがなされているかどうかの判断を監査役に求めている。したがって、“IT リスク”を踏まえた IT 管理の全般的な体制とその運用状況に対する監視と検証に留意する必要がある。



Q13：事業継続管理にはどう関与すべきか？

Q 東日本大震災を受けて、当社でも事業継続計画（BCP）の見直しをしています。当社は、EMS との受発注システムの運用を行っており、今回の大震災時にその効果を発揮しましたが、その反面、システムのダウンは即事業活動の停止に繋がってしまいます。監査役としても BCP の改訂に何らかのかたちで関与すべきと考えていますが、具体的にどのような点を確認、検証すればよいのでしょうか？

A 監査すべき視点としては、①リスクに対する事前準備ができており、あらかじめ自社のリスクを抽出し評価した上で、対応策ができているか、対応策は定期的に見直されているか、②リスク発生時の対応として、災害の発生により事業継続に支障がでた場合、迅速で的確な対応がとられ、被害の拡大を防止する対策がとられているか、③被害を受けた事業の早期復旧計画が策定されているか等が、ポイントとなります。

東日本大震災での事例を見てみますと、外部電源が断たれたため、社内サーバーがダウンし社内システムが止まってしまった会社が多かったようです。そのため自家発電装置を購入したり、賃借手配に走った会社が多く、会社によっては計画停電時に社内システムの利用を制限したところもあったようです。このようなことが起きないよう、監査役として次の点を普段から監視し検証しておく必要があると思われます。

- 外部電源が断たれた場合の対策（非常電源装置、自家発電装置等の備置）
- サーバーの設置場所（社内、社外の専門データセンター等）
- バックアップデータの外部保管場所

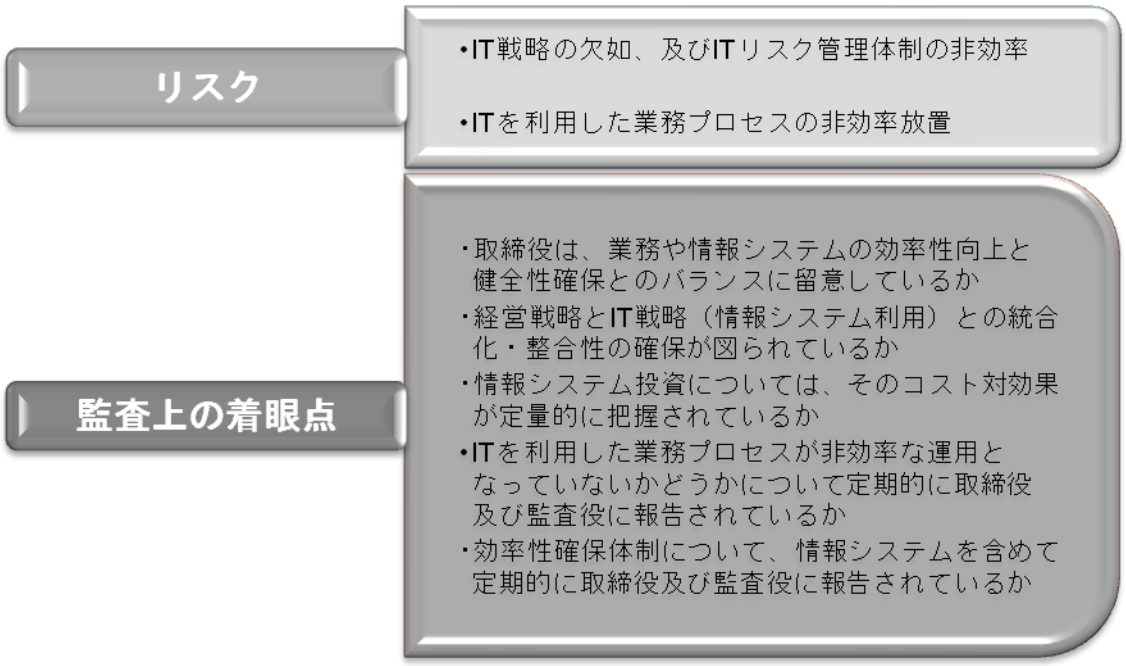
③効率性確保体制の監査

IT の利活用は、効率性の追求を目的とすることが多いため、その目的が達成されているかどうか、あるいは過度の効率性追求が経営リスクにつながっていないかどうかという視点が必要である。

「内部統制システムに係る監査の実施基準」（第 11 条）でも、この点に関連して、「経営戦略の策定、経営資源の配分、組織の構築、業績管理体制の構築・運用等が適正に行われない結果、過度の非効率性が生じ、その結果、会社に著しい損害が生じるリスク」及び「過度の効率性追求により会社の健全性が損なわれ、その結果、会社に著しい損害が生じるリスク」を挙げている。

したがって、監査役は、取締役が企業経営の健全性確保とのバランスに留意した IT の利活用を行っているかどうかを監視し検証する必要がある。

なお、「実施基準」では、経営計画の策定等と並んで、「IT への対応」が適正に決定・実行・是正される仕組みの構築・運用を、重要な統制上の要点としている点に留意すべきである。



Q14：IT 投資の監査ポイントとは？

Q IT 戦略の監査にまで踏み込もうとするとき、その裏側にある IT 投資の中身にまで立ち入る必要があるように思えます。IT 投資については、投資対効果が見えにくく、追加投資が増大することが多いとも聞きます。IT 戦略との関係で IT 投資を監査している事例はありますか？

A 当社では、次のようなポイントで監査を実施しています。

・IT 戦略に基づき、中長期及び単年度の IT 投資計画が策定されているか。また、計画の内容は IT 戦略と整合性がとれ、予算規模も適切か。

・IT 投資計画の策定及び個別投資の決定にあたっては、情報システム部門、ユーザ部門及び経理・企画等調整部門との間で、十分に検討され、協議されているか。

・投資の内容は、業務や情報システムの効率性向上と健全性確保とのバランスが図られているか。コスト対効果が適切に把握されているか。

・ベンダー選定のプロセスが確立されているか、プロセスの内容は適切か。

・システム開発のプロセスが確立されているか。開発の進捗状況をモニタリングし、必要な意思決定を行える体制が整備されているか。

IT 投資も他の投資案件と同じように監査すればよいのですが、システム開発は長期に亘ることがしばしばですので、四半期ごと等に取締役会で進捗状況のヒアリングをする等のきめ細かい対応が必要になる場合もあります。

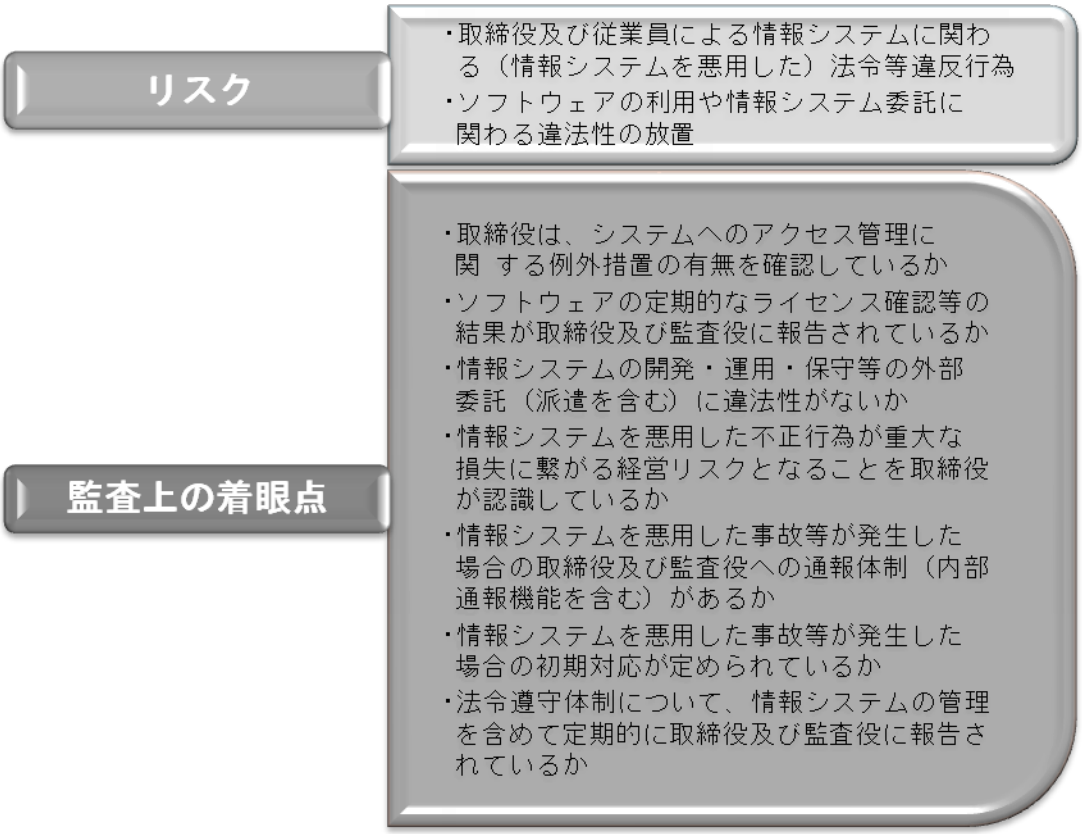
また、システム開発が長期化すると、途中の経過が見えにくくなることがあるので、追加的な投資コストを避けるためにも、計画に沿った開発が行われていることや、特にユーザと開発者の間に仕様のギャップがないかのチェックもあわせて必要です。一旦、システム開発をスタートすると途中で中止することは難しく、気がつくと初期投資の２～３倍に膨れ上がってしまう実例が散見されますので、注意が必要です。

④法令等遵守体制の監査

ソフトウェアの著作権、情報システムを使った個人情報の取扱い、システム開発に関わる外部委託先の監督、システム開発に従事する派遣社員の管理、さらには従業員等による不正アクセスなどに関連して、IT の利活用においても、さまざまな法令等違反のリスクが潜んでいる。

「内部統制システムに係る監査の実施基準」（第８条）でも、取締役等が主導又は関与する法令等違反行為はもとより、「法令等遵守の状況が代表取締役等において適時かつ適切に把握されていない結果、法令等違反行為が組織的に又は反復継続して行われるリスク」を挙げている。

したがって、監査役は、取締役が法令等違反行為として IT の利活用にも留意し、法令等の遵守に関わる方針や行動基準等を定めて周知徹底しているとともに、その状況が内部監査部門等によってモニタリングされ、問題点の発見と改善措置がとられていることを監視し検証する必要がある。



Q15：IT 利活用の法令違反のケースとは？

Q 監査役の立場としては、まずもって法令違反の有無に気をつかいますが、IT の利活用に関して、具体的にどのようなケースがありますか。

A まず挙げられるのは、ソフトウェアの違法コピー問題です。権利者から実施許諾されていない違法コピーが社内で使用されていると著作権法違反に該当し、10 年以下の懲役もしくは 1 千万円以下の罰金又は併科となり、法人が主導した場合は、法人への罰金の上限が 3 億円に引き上げられています。IT 担当部署と協力して、定期的に社内で違法コピーが使用されていないかどうかを確認しておく必要があります。

次に気をつけなければならないのは、情報漏洩問題です（情報漏洩対策のための監査については Q12 を参照）。IT は各種機密情報と客先等の個人情報の管理に密接に関係し、IT の利活用なしにはこれらの情報管理は不可能といっても過言ではありません。それだけに管理の徹底が望まれます。情報漏洩問題が発生すると、契約に基づく損害賠償責任が、また個人情報保護法に基づく個人情報取扱事業者としての責任が問われる可能性があります。

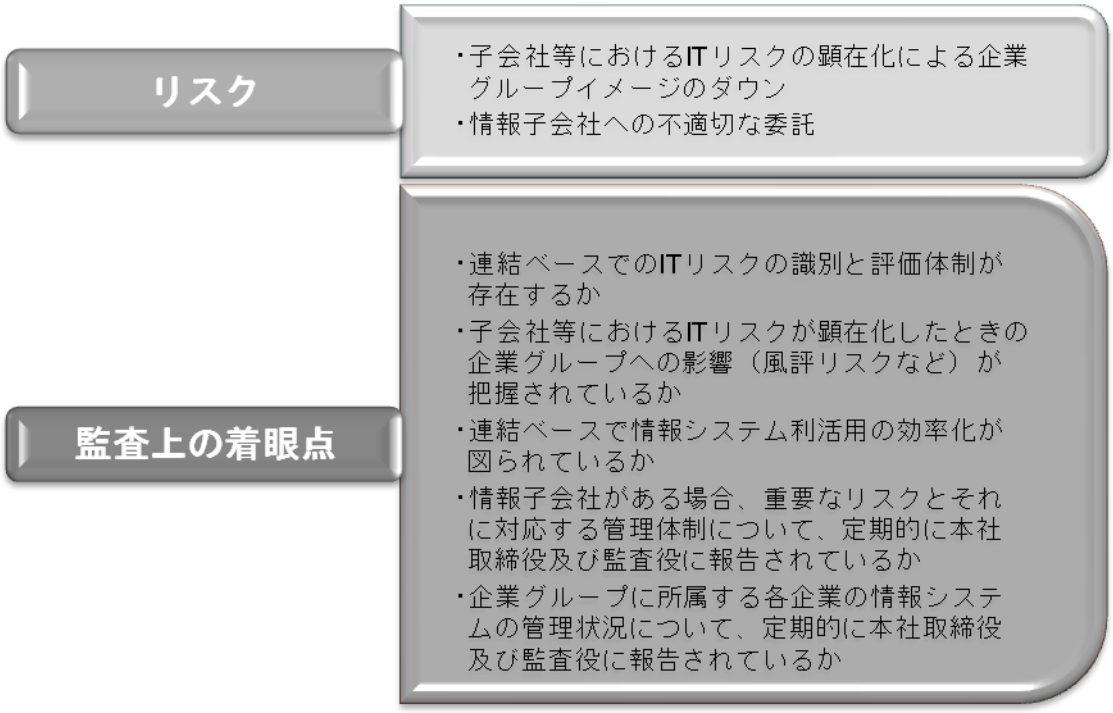
この他にも、ネット上の不正アクセスを禁止する不正アクセス禁止法、システム開発等に従事する派遣社員の労働環境を規定する労働者派遣法、電子署名及び認証業務を規定する電子署名法等がありますので、必要に応じ主管部署にその内容を確認してください。

⑤企業集団内部統制の監査

IT の利活用を効果的かつ効率的に行い、かつ、IT 管理を徹底するためには、企業グループ全体としての統一のとれた取組みが必要となる。子会社で起こった個人情報漏洩等の情報システムに関わる事故が、企業グループ全体のイメージを大きく損ねることもある。また、情報システムの企画・開発・運用・保守を、情報システム子会社に委託している場合には、当該情報子会社を対象とした監査が必要となってくる。

「内部統制システムに係る監査の実施基準」（第 12 条）でも、「重要な子会社において法令等遵守体制、損失危険管理体制、情報保存管理体制、効率性確保体制に不備がある結果、会社に著しい損害が生じるリスク」及び「重要な子会社における内部統制システムの構築・運用の状況が会社において適時かつ適切に把握されていない結果、会社に著しい損害が生じるリスク」を挙げている。

海外子会社の場合には、地理的条件から管理の目が行き届きにくいことにくわえ、文化や風土等の違いからコンプライアンス意識が日本の場合と異なることも少なくないため、特に留意する必要がある。



Q16：子会社の情報管理のあり方とは？

Q　これまでの事例をみる限り、情報漏洩等の事故の多くは、子会社で起こるケースが多いようにも聞きます。管理の強化と効率性から、IT システムを親会社のシステムで統一化しようとしていますが、高額などの理由で対応してもらえません。監査役として、どのような対応が望ましいでしょうか？

A　企業集団の IT 統制の観点からは、IT システムはグループとして同一システムを導入するのが理想でしょう。しかしながら、会社の規模等から親会社で使用するシステムが子会社で適切であるとは限りません。

内部統制の観点も踏まえ、グループとしての統一性に留意し、子会社主管部門が中心となり、関連部門、内部監査部門と協議し、望ましい IT リスク管理体制の方向性を打ち出すべきと考えます。監査役はこの検討過程をレビューし、必要に応じ監査法人の意見も徴し、その方向性を検証することが必要です。

しかしながら、最終的に子会社で別システムを採用することとなっても、データの変換などにより、グループとしての統一性に留意した、システムの選定が必要です。

（２）「金融商品取引法」に基づく取組みのポイント

① 内部統制に対する監査役の目線

上場会社にあっては、金融商品取引法に基づいて、財務報告に係る内部統制の評価と監査が義務づけられている。

金融庁・企業会計審議会の「財務報告に係る内部統制の評価及び監査の基準」では、「監査役又は監査委員会は、取締役及び執行役の職務の遂行に対する監査の一環として、独立した立場から、内部統制の整備及び運用状況を監視、検証する役割と責任を有している」とされている。

この制度では、内部統制の基本的要素として「IT への対応」が明記され、財務報告につながる情報システムについては、経営者による評価と公認会計士・監査法人による監査が求められている。

監査役としてこの制度に対応する場合、経営者による評価の妥当性判断と、公認会計士・監査法人による監査の妥当性判断が必要となるが、まずもって重要な視点は、図７に示すように、内部統制報告制度が前提とするのは、あくまでも「財務報告」に関係する内部統制に過ぎないという点である。

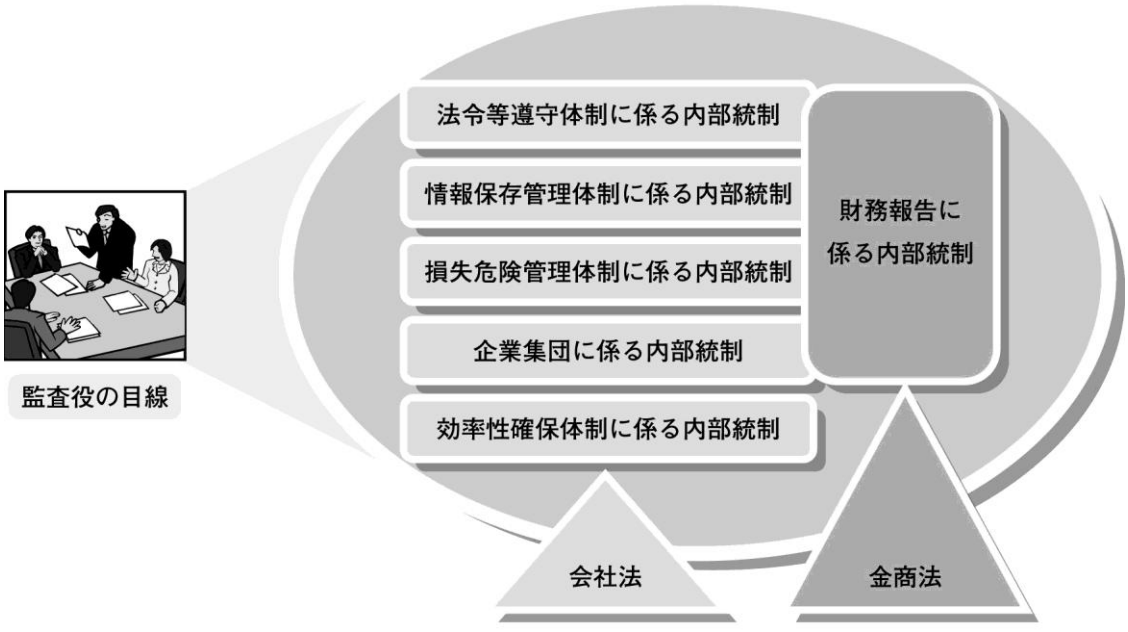


図７　２つの内部統制への対応

「決算プロセスにつながる内部統制によって適正な財務報告はできたが、当該制度がカバーしない領域で個人情報の漏洩事故が起こり多額の損害賠償の負担とともに会社の評判を大きく失墜したとか、大規模災害によって事業・業務の継続が困難になったとか、業務の非効率さがいつまでたっても改善されない」といったことは、起こり得る。金融商品取引法でいう内部統制は、会社法が想定する内部統制よりもその範囲が狭いのである。会社法施行規則でいう「効率性確保体制の内部統制」は、金融商品取引法の内部統制報告制度がカバーする範囲外である。また、その他の会社法施行規則でいう内部統制も、財務報告に関わる部分はきわめて限られている。

IT についても、「財務報告に係る内部統制の評価及び監査の基準」で「IT への対応」が明記されたからといって、すべての IT リスクに対応しているわけではない。

したがって、監査役は、「財務報告に係る内部統制」だけを取り出して近視眼的に見るのではなく、まずもって会社法が想定する広義の内部統制やリスク管理に対する目線をもち、その全体の中で財務報告に係る内部統制に対応することが重要である。

②「IT への対応」の全体像と監査役監査のポイント

「財務報告に係る内部統制の評価及び監査の基準」でいう「IT への対応」は、図８に示したように、「IT 環境への対応」と「IT の利用及び統制」からなっている。

「IT 環境への対応」とは、企業の事業・業務活動に関わる企業内外の IT の利用状況のことであり、「IT の利用及び統制」に影響を及ぼす環境要因をいう。

また、「IT の利用及び統制」とは、統制環境、リスクの評価と対応、統制活動、情報と伝達、モニタリングという内部統制の構成要素の有効性を確保するために、IT を有効かつ効率的に利用すること、及びその利用のための方針と手続をいう。

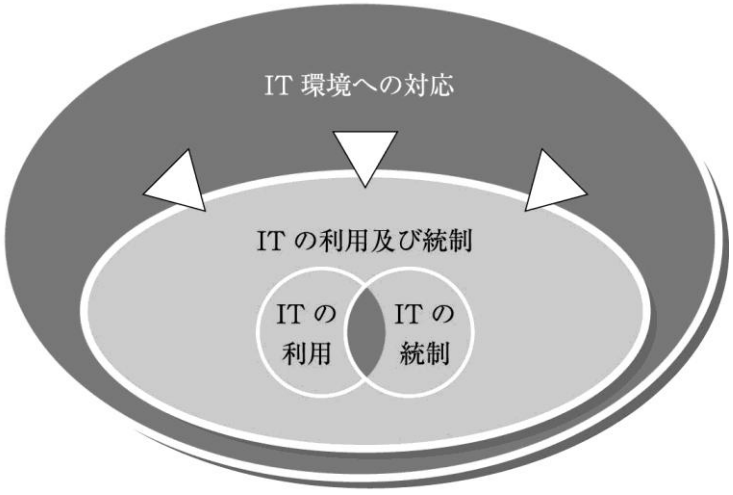


図８ 「IT への対応」の構成内容

③「IT の利用及び統制」の内容

「IT の利用及び統制」は、次のような内容からなっている。

＜IT の利用＞

- 統制環境に関わる利用例
  →IT 教育等を通じた全社的な IT 活用能力の向上
- リスク評価と対応に関わる利用例
  →IT を活用した厳密なリスク評価やリスク情報の共有
- 統制活動に関わる利用例
  →統制活動の自動化による人的ミスの回避や統制手続の効率向上
- 情報と伝達に関わる利用例
  →IT による情報の共有と適時な伝達
- モニタリングに関わる利用例
  →モニタリングの自動化による効率向上

＜IT の統制＞

- IT 全般統制
  ・システムの開発、保守に係る管理
  ・システムの運用・管理
  ・内外からのアクセス管理などのシステムの安全性の確保
  ・外部委託に関する契約の管理
- IT 業務処理統制
  ・入力情報の完全性、正確性、正当性等を確保する統制
  ・例外処理（エラー）の修正と再処理
  ・マスターデータの維持管理
  ・システムの利用に関する認証、操作範囲の限定などのアクセスの管理

監査役は、これらの全てに精通している必要はなく、IT 全般統制や IT 業務処理統制の細々とした評価に関与する必要はない。たとえば、アクセス管理の技術的な評価に気をとられていて子会社（情報子会社・関連会社を含む）の管理や委託先への管理に重大な問題があったというのでは、監査役として十分な役割を果たしたとは言えないであろう。

監査役は、まず IT が利用されている状況を把握し、その上で、IT が内部統制目的に効果的に利用されているかどうか、また IT による情報システムにリスクに応じた統制が組み込まれているかどうかを大局的に見極めることが重要である。

企業会計審議会の「財務報告に係る内部統制の評価及び監査に関する実施基準」で「IT に係る全社統制」として示された以下の評価項目が、監査役として確かめておくべきポイントと理解してよいであろう。

- 経営者（取締役）は、IT に関する適切な戦略、計画等を定めているか。
- 経営者（取締役）は、内部統制を整備する際に、IT 環境を適切に理解し、これを踏まえた方針を明確にしているか。
- 経営者（取締役）は、信頼性のある財務報告の作成という目的の達成に対するリスクを低減するため、手作業及び IT を用いた統制の利用領域について、適切に判断しているか。
- IT を用いて統制活動を整備する際には、IT を利用することにより生じる新たなリスクが考慮されているか。
- 経営者（取締役）は、IT に係る全般統制及び IT に係る業務処理統制についての方針及び手続を適切に定めているか。

Q17：JSOX における IT の開示すべき重要な不備の事例は？

Q 金融商品取引法に基づく、財務報告に係る内部統制の評価及び監査において、IT に関係する「開示すべき重要な不備」（2011 年３月以前は「重要な欠陥」という用語）の事例というのはあったのでしょうか？

A 情報システムを原因とする開示すべき重要な不備（重要な欠陥）は、比率からするとそれほど多くはありませんが、内容的には会計データの一部消失というケースがあり、その放置は財務報告の適正性を大きく揺るがす問題に直結します。以下は、IT 関係が原因となって財務報告に係る内部統制が有効でないと判断された経営者評価結果（内部統制報告書）の該当部分の抜粋です。

当社では、システムの保守及び運用の管理を適正に行うため、「運用・保守管理規程」を定めて遵守することが義務付けられているが、コンピュータデータの保全手続きにおいて、当該規程の運用が不十分であったため、会計データの一部が消失し、当期の財務諸表作成にあたって消失したデータの修復作業を行うこととなった。

事業年度の末日までに是正されなかった理由は、上記会計データのバックアップデータ復元作業のテスト実施が十分でなく、バックアップデータ消失のリスクを予見できなかったためである。

＊有価証券報告書から引用：なお、社名は伏せてある。

３．災害対応と IT ガバナンス

（１）IT ガバナンスと IT サービス継続の関係

事前の手当てがなく地震等の災害に見舞われたとき、

- 情報システムが組み込まれている事業活動や業務活動の水準が急激に落ち込んだり、最悪の場合には完全停止する
- IT や情報システムによって処理・保存されているデータや情報が入手又は提供できない、あるいはデータベース上のデータが壊れてしまう

といった事態に陥る可能性がある。

そこでこのような地震等の自然災害に起因する IT リスクに対しては、大別して、以下の３つの対策が必要となる。

- 災害に対して被害を最小限に食い止めるための**「予防対策」**
- 災害が発生したときにもっとも適切な対応（被害を可能な限り小さくし、二次被害を防ぐとともに、可能な限り早い復旧を目指す）をとるための**「災害時対策」**
- あらかじめ復旧目標を定めて元の状態に復元・復旧するための対応をとるための**「復旧対策」**

この３つの対策は「全社的災害プログラム」（最近では、事業・業務活動の継続性確保に焦点を当てて、BCP と呼ばれることが多い）として統合して策定される必要があるが、事業・業務活動が IT や情報システムに大きく依存している場合には、全社的プログラムの中には「IT サービスを継続するためのプログラム」が組み込まれていなければならない[7]。

取締役は、災害によって IT や情報システムが大きな被害を受けた場合、最悪、企業活動がストップすることも想定しておく必要がある。その上で、適切な対策を講ずることは取締役としての責務である。

したがって、監査役は、自社の IT や情報システムの重要性等に基づいて、災害によって被害を受けた場合に事業・業務活動に及ぼすリスクを、取締役が十分に理解した上で、適切な対策を講じているかどうかを監視し検証しなければならない。

---

[7] 「災害リスクマネジメント・プラン」という場合には主に「予防対策」に重点が置かれ、また「コンティンジェンシー・プラン」という場合には「緊急時対策」に、さらに「ディザスター・リカバリー・プラン」という場合には「復旧対策」に重点が置かれる。いうまでもなく予防対策、緊急時対策、復旧対策はそれぞれが結び付けられている必要があるので、「xxx プラン」という場合、その名称によってどこに重点が置かれるかによる違いとして理解するのがよいであろう。また、最近よく耳にする「BCP」とか「BCM」というのは、天災、人災、不正等のリスクの原因事象を問わず、事業・業務活動の継続性をいかに確保するかという観点からする対策である。IT や情報システムの機能停止や機能低下は、災害だけでなく、外部からの攻撃、過重負荷、コンピュータ・ウィルスの感染、ハードウェアやネットワークの故障などによっても起こるので、原因別の対策を考えるのではなく、IT や情報システムのサービス停止時間を少しでも短くすることで IT サービスの継続を図るという観点から策定される。

IT サービスの継続性確保は事業・業務継続の一部分である。その一方で、IT サービスの継続性を確保するためには相当な投資を必要とし、企業グループ（場合によってはサプライチェーンを構成する企業群）全体として取り組むべき課題であるから IT ガバナンスの一部分に位置づけられる。この関係を図示したものが図９である。

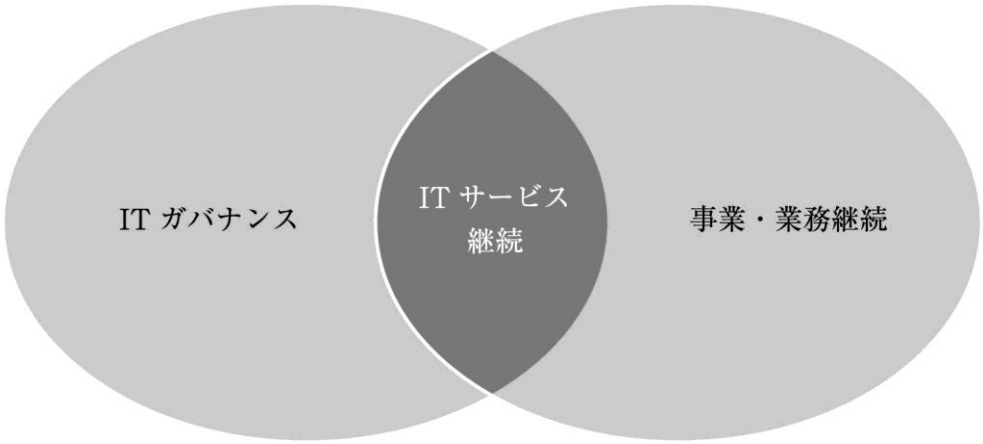


図９　IT ガバナンス、事業・業務継続、IT サービス継続との関係

〈注〉なお、作図に際しては、経済産業省「IT サービス継続ガイドライン」を参考とした。

（２）想定される被害と事業・業務継続の関係

監査役は、策定された「BCP」、「コンティンジェンシー・プラン」、「ディザスター・リカバリー・プラン」、あるいは「IT サービス継続プログラム」といったものを微に入り細にわたり検証する必要はない。かといって、これらが確かに策定され、文書化されていることを確かめるだけでは不十分である。

監査役は、図 10 に例示したように、IT や情報システムへの想定される被害によって、事業・業務活動にいかなる影響を及ぼすか（ビジネス・インパクト分析という）を取締役が十分に把握し、理解しているかをまずもって見極めておくことが重要である。

社内又は企業グループとしての「購買－生産－物流－販売」の一連の主要な事業活動は密接に関連づけられていることから、IT や情報システムへの想定される被害が生じたときに、どこがボトルネックになるかが把握されていなければならない。

東日本大震災では、社内事業プロセスの前提となる企業間のサプライチェーンの途絶が事業活動の継続にとっての障害となるケースが多々生じた。部品の供給を受けられないといった物理的な流通障害とともに、企業間のサプライチェーンを支える IT や情報システムも甚大な被害を受け、必要な情報が適時にやり取りできないといった問題も表面化するところとなった。いまや IT や情報システムは企業間のサプライチェーンのサポートにとって必須の手段となっており、流通ルートの確保とともに、IT のサービス継続の重要性が見直されている。

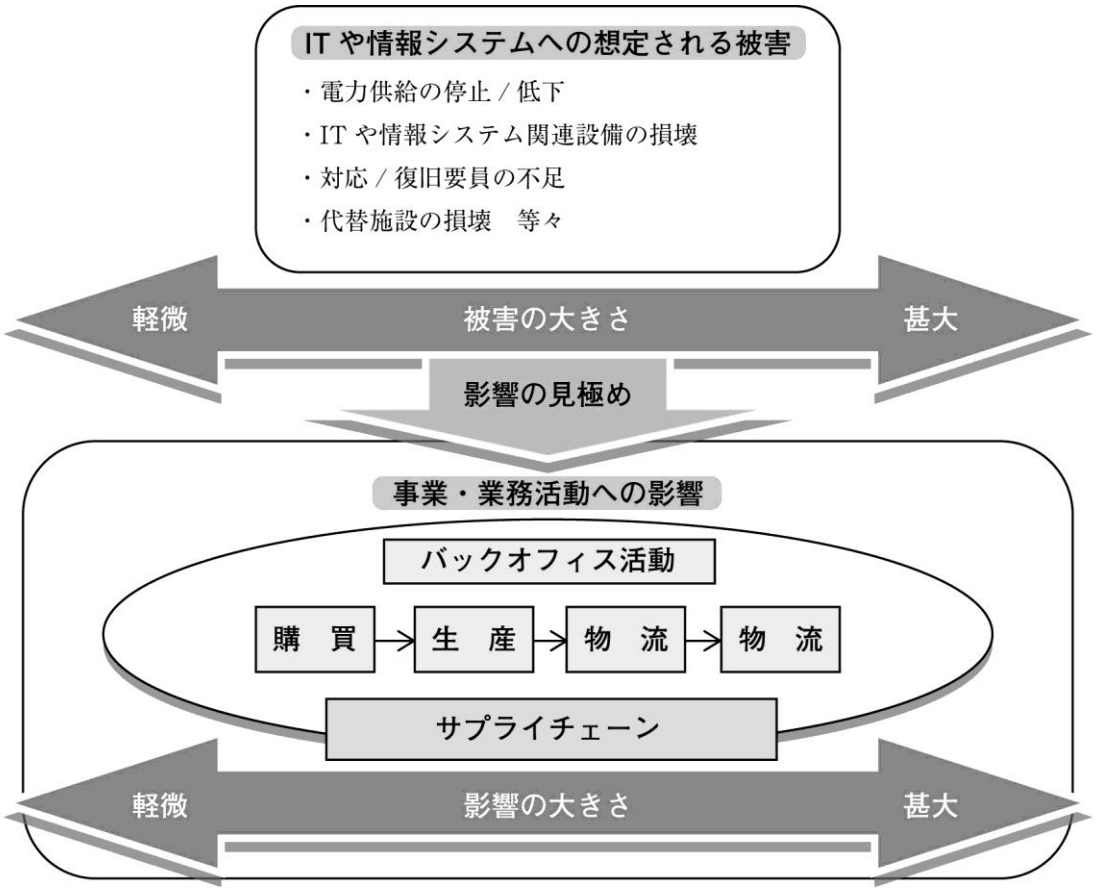


図 10　IT や情報システムへの想定される被害とその影響分析

（3）監査役が質問すべき事項（見落としがちなポイント）

☑	IT に関わる BCP 監査のチェックポイント
	複数の BCP が作成されている場合、IT や情報システムという観点から整合性が取られているか
	情報システム部門だけでなく組織横断的な観点から、IT サービス継続のための対策が計画されているか
	事業・業務活動の重要性（顧客サービスにとっての重要性を含む）によって復旧すべきアプリケーションの優先順位が明確になっているか
	情報システムやデータのバックアップの損壊、通信ネットワークの迂回路の損壊まで想定しているか
	情報システムの運用・保守の外部委託先の罹災まで想定しているか
	システム構成の変更やソフトウェアの改修等があった場合に BCP が適時に見直されているか
	災害時のセキュリティ水準の低下が想定されているか
	外部のステークホルダー（取引先を含む）への適切な情報開示が行われているか

＜付録＞

「会社法施行規則」に基づく ITガバナンス・チェックリスト

本付録は、本文第Ⅱ部「2．内部統制システム構築に即した取組みのポイント」の「（1）「会社法施行規則」に基づく取組みのポイント」より「監査上の着眼点」を抜粋し一覧に整理したもので、監査役監査のチェックリストの一例として作成したものである。

＜付録＞「会社法施行規則」に基づくITガバナンス・チェックリスト

番号	項目	結果
	１．情報保存管理体制の監査	
1	重要情報が漏洩した場合のリスク、及びそれに対応する管理方針が取締役会において議論されているか	
2	セキュリティポリシー（個人情報保護方針を含む）が策定され、組織内に周知徹底されているか	
3	情報及び情報システムへの適切なアクセス管理体制がとられているか	
4	情報及び情報システムのバックアップとリカバリー体制は十分か	
5	情報漏洩事故等が発生した場合の取締役及び監査役への通報体制（内部通報機能を含む）があるか	
6	情報保存管理体制について、情報システムの管理を含めて定期的に取締役及び監査役に報告されているか	
	２．損失危険管理体制の監査	
7	取締役がITリスクを経営リスクとして認識しているか	
8	重要なITリスクの識別と把握が取締役会において行われているか	
9	リスク管理体制の一環として情報システムに係るリスク管理体制が含められているか（事業継続計画等を含む）	
10	ITリスク管理体制の運用状況について定期的に取締役及び監査役に報告されているか	
11	ITリスクが顕在化した際の初期対応が定められているか	
12	損失危険管理体制について、情報システムの管理を含めて定期的に取締役及び監査役に報告されているか	
	３．効率性確保体制の監査	
13	取締役は、業務や情報システムの効率性向上と健全性確保とのバランスに留意しているか	
14	経営戦略とIT戦略（情報システム利用）との統合化・整合性の確保が図られているか	
15	情報システム投資については、そのコスト対効果が定量的に把握されているか	
16	ITを利用した業務プロセスが非効率な運用となっていないかどうかについて定期的に取締役及び監査役に報告されているか	
17	効率性確保体制について、情報システムを含めて定期的に取締役及び監査役に報告されているか	
	４．法令等遵守体制の監査	
18	取締役は、システムへのアクセス管理に関する例外措置の有無を確認しているか	
19	ソフトウェアの定期的なライセンス確認等の結果が取締役及び監査役に報告されているか	
20	情報システムの開発・運用・保守等の外部委託（派遣を含む）に違法性がないか	
21	情報システムを悪用した不正行為が重大な損失に繋がる経営リスクとなることを取締役が認識しているか	
22	情報システムを悪用した事故等が発生した場合の取締役及び監査役への通報体制（内部通報機能を含む）があるか	
23	情報システムを悪用した事故等が発生した場合の初期対応が定められているか	
24	法令遵守体制について、情報システムの管理を含めて定期的に取締役及び監査役に報告されているか	
	５．企業集団内部統制の監査	
25	連結ベースでのITリスクの識別と評価体制が存在するか	
26	子会社等におけるITリスクが顕在化したときの企業グループへの影響（風評リスクなど）が把握されているか	
27	連結ベースで情報システム利活用の効率化が図られているか	
28	情報子会社がある場合、重要なリスクとそれに対応する管理体制について、定期的に本社取締役及び監査役に報告されているか	
29	企業グループに所属する各企業の情報システムの管理状況について、定期的に本社取締役及び監査役に報告されているか	