研究ノート

システム監査の視点からの企業ガバナンスの一考察

A Study of Corporate Governance from the Viewpoint of Systems Audit

松田　貴典
Yoshinori Matsuda
大阪成蹊大学
Osaka Seikei University

概　要

企業で不祥事が発生すると、それは「ガバナンスの問題である」とか「ガバナンスが効いていない」などと指摘される。そこで、企業ではガバナンスをどのように考え、どのような管理・統制機能が設置され、位置付けされて確立（実行）されているのか、調査し考察した。調査にあたっては、主要な業種を代表する企業を Web から検索し、ガバナンスの位置付けや管理・統制機能関連のフレームワーク図を作成し俯瞰的な視点で考察した。その一方で、ガバナンスと密接に関係する IT ガバナンスと情報セキュリティガバナンスについても企業の Web 情報から調査し、監査の状況についても考察した。ガバナンスについては、個別の管理・統制機能をテーマにした研究は多いが、組織全体から見た管理・統制機能の位置付けやフレームワーク図からの調査研究は少ない。

キーワード：ガバナンス　IT ガバナンス　情報セキュリティガバナンス、フレームワーク　監査

1．はじめに

企業で不祥事が発生すると、それは「ガバナンス（Governance）の問題である」とか「ガバナンスが効いていない」などと指摘される。一般的に、ガバナンスは、企業における不正行為や経営陣の暴走を防ぐための管理・統制する仕組みや牽制機能を指す「コーポレートガバナンス[注1]」を意味している。そして、経営陣による経営の私物化や不正を防ぐこと、また、企業の不祥事を防ぐことを目的として、組織等で方針やルールなどを決めて、組織内に指示徹底し実行させることである。さらに、ステークホルダー（Stakeholder: 株主などの利害関係者）が、企業の経営を監視することになる。実用日本語辞典によれば、『ガバナンスとは、主に「統治」「支配」「管理」と和訳され、少なからず「地位の高い者が組織をうまく取り仕切る」という意味合いを含んでいる。ただし、上から下への一方的に支配という意味合いよりは、組織や社会に所属する当事者たちが、意思決定に携わる「自治」のニュアンスが強い。コーポレートガバナンスという語もこの意味合いを前提とする使い方がされている。』としている[1]。

企業では、これまで、不祥事を起こすと、社会的な評価や企業への影響をできるかぎり少なくするために、経営者自ら謝罪し、組織改革やガバナンス改革を実行してきた。例えば、CSR（Corporate Social Responsibility: 企業の社会的責任）、コンプライアンス（Compliance: 法令遵守）、リスクマネジメント、内部統制などは組織改革や組織統制等に使われた用語である。その一方で、事業継続管理や環境問題への対応としてのサステナビリティ（Sustainability: 持続可能性）など次々に改革が求められて、新たな改革が生まれてきた。

しかし、実際に、企業ではガバナンスの中に、どのような管理・統制機能が位置付けされて、確立（実行）されているのか、また、ガバナンスの概念が、どのように考えられているのか、企業全体としての管理・統制機能の位置付けが、分かりに

投稿受理日	2019 年 4 月 15 日
再投稿受理日	2019 年 5 月 23 日
査読完了日	2019 年 5 月 27 日

くい。そこで筆者は、主要な業種を代表する企業をWebから検索して、ガバナンスの位置付けや管理・統制機能関連のフレームワーク図（以後、「管理統制フレームワーク」と言う。）を作成し、俯瞰的な視点で考察した。これらの調査や分析により企業のガバナンスに対する考え方や理念、社会に対する行動指針、さらに、セキュリティやリスク管理の対応など、様々な管理・統制機能を知ることができた。

一方、経済産業省は、平成30年4月20日にシステム監査を実施する監査人の行為規範及び監査手続きの規則を規定した「システム監査基準」、システム監査人の判断尺度を規定した「システム管理基準」を改訂し、公表した。これまでの基準が平成16年10月に改訂であったことから、実に14年経過の改訂である。

今回の改訂のポイントの一つは、ITガバナンスの実現ための実践行動を起こすことを明確にしたことである。これまでのシステム管理基準においても、ITガバナンスの概念や事業継続計画（BCP:Business continuity planning）を定めていたが、これまで以上に、明確化し実現を求めた背景には、ITガバナンスについてのJIQ38500や事業継続計画についてのJISQ22301等の国際基準の制定や、米国におけるCOBITなどとの整合性をとるためであった。特に、新たなシステム管理基準では、その主旨で、「情報システムにまつわるリスクを適切にコントロールしつつ、これまでの以上にITガバナンスの実現に貢献する」と明記されたことは、重要なことである。

システム管理基準の枠組みの中で、ITガバナンスの必要性について、「ITガバナンスを実践する上で、情報システムにまつわるリスクだけでなく予算や人材といった資源の配分や、情報システムから得られる効果の実現にも十分に考慮する必要がある。」としている。ITガバナンスの確立に向けた原則や組織体制及び実践すべき行動基準となる管理基準の内容が20頁に渡って示されている[2]。

しかし、調査した企業のガバナンスの中には、ITガバナンスは、明示的に位置付けされていない場合が多く、また、その確立を支援し担保する監査（システム監査を含む）については、ほとんど記述はされていない。

そこで、筆者は、情報システムのガバナンス（ITガバナンスや情報セキュリティガバナンス）についても、公開されている資料等を参考に、その位置付けや管理・統制機能について考察した。

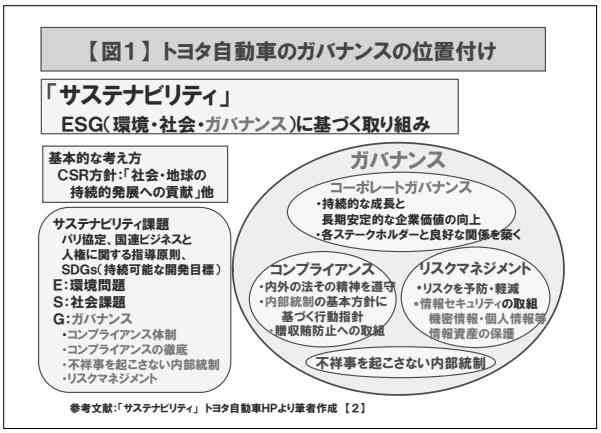
2．事例からみる企業のガバナンスと管理統制フレームワーク

企業のガバナンスの考え方を知る手がかりとして、まず、ガバナンスについて記載内容や、全社的な管理統制フレームワークから見ることが重要である。企業の管理統制フレームワークには、統一した理論があるわけではない。むしろ、企業の業種や企業理念・方針等によって管理統制フレームワークが構成されると言える。

一方、情報システムが高度化することで、ガバナンスに関連する情報システムのガバナンスについても調査した。情報システムのガバナンスには、その中核をなすITガバナンスと情報セキュリティガバナンスがあり、ガバナンスとどのように関連付けされているかについても調査した。本稿で検討した企業は、代表的な自動車メーカ、情報テクノロジー企業、金融機関である。

①大手自動車メーカの「トヨタ自動車」【図1】

日本を代表する自動車メーカのトヨタ自動車におけるガバナンスは、「サステナビリティ」の下で掲げられている。最初に記載されている取り組み姿勢の文章には、『未来がよりよい社会となるように、「環境」「社会」を重要な課題と考えています。また、お客様に信頼され続ける会社でありたい。こうした思いで、「ガバナンス・コンプライアンス・リスクマネジメント」に取り組みます。』と書かれている。トヨタ自動車のガバナンスの考え方は、自動車業界のリーダーとして、社会と共に成長することを念頭において事業活動をしており、ステークホルダーから信頼され続けることを最重要課題としていることである。この期待を踏まえてサステナビリティ課題として特定している。サステナ



ビリティ課題の特定にあたっては、事業を取り巻く環境を「パリ協定」「国連ビジネスと人権に関する指導原則」「SDGs (Sustainable Development Goals: 持続可能な開発目標)」など、国際的に合意された規範を踏まえ、企業価値の向上と経営基盤の強化、リスクマネジメントの両面から検討されている。

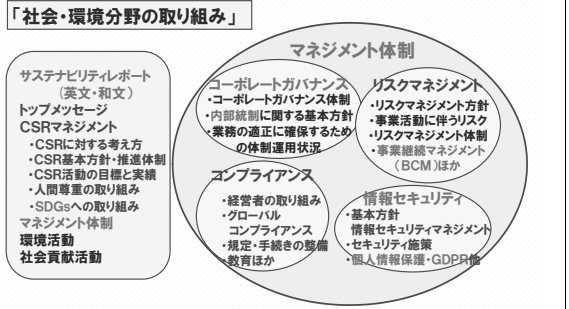
その上で、サステナビリティ課題として、ESG を掲げている。ESG は、それぞれ環境(Environment)、社会（Social)、ガバナンス(Governance）の頭文字であり、ESG の取組みは優れた企業の証となる。社会の発展に貢献し、将来に渡って持続的に成長するという考え方が根底にある。また、ガバナンスの中に、経営を揺るがすリスクの未然防止を目的に、「コーポレートガバナンス」「コンプライアンス」「リスクマネジメント」とともに、「不祥事を起こさない内部統制」を掲げている[3]。

②大手テクノロジーの企業の「富士通」【図2】

富士通はテクノロジーをベースとしたグローバル ICT（Information and Communication Technology）企業である。富士通は、「地球と社会の持続可能発展に貢献」をテーマに、「社会・環境分野の取り組み」の中のマネジメント体制において、「コーポレートガバナンス」「コンプライアンス」「リスクマネジメント」「情報セキュリティ」を掲げている。また、「地球と社会の持続可能発展に貢献」の中では、「CSR マネジメント」「環境活動」「社会貢献活動」なども掲げており、持続可能な発展をめざした「サステナビリティ」が重要な取り組みとなっている。前述のトヨタ自動車と特徴的な違いは、マネジメント体制のなかで、「情報セキュリティ」を掲げていることである。情報セキュリティがテクノロジー企業として、重要な取り組みであることを示している。

コーポレートガバナンスの中で、内部統制に関する基本方針が示されており、企業価値の持続的向上を図るための経営効率化の追求、事業活動で生じるリスクコントロールの重要性を示している。その内容では、業務執行の決定と執行体制、リスクマネジメント体制、コンプライアンス体制の整備が図られている。リスクマネジメント体制では、製品・サービスの欠陥や瑕疵に関するリスク管理体制、受注プロジェクトの管理体制、セキュリティ体制及び財務上のリスク管理の整備を図っている。また、リスクマネジメントのプロセスでは、事業活動に伴うリスクの抽出・分析・評価を実施し、重要なリスクに対する回避・軽減・移転・保有などの対策状況を確認した上で、①リスクマネジメントの方針・プロセスの決定、②プロセスの実践、③モニタリング・見直し、④継続的改善のマネジメントサイクルが実施され、定期的に取締役会に報告されている。

【図2】富士通のガバナンスの位置付け



参考文献：「社会・環境分野の取り組み」「マネジメント体制」富士通HPより筆者作成【3】

リスクマネジメント体制とコンプライアンス体制は、「内部統制体制の整備に関する基本方針」での中心的な位置付とされており、具体的には「リスク・コンプライアンス委員会」を設置し、取締役会の直属組織となっている。この委員会の中に CISO（Chief Information Security Officer: 最高情報セキュリティ責任者）を置き、情報セキュリティ施策の策定と実行を行っている。また、該社は、ICT を基幹業務としており、「快適で安心できるネットワーク社会づくり」への貢献を企業理念としている。そこで、マネジメント体制の中では、「情報セキュリティの確保」を重点課題としており、ICT ビジネスを支える情報セキュリティガバナンスの強化を図っている。情報の保護を目的とする「情報管理」、サイバー攻撃に対するシステム防御施策の「サイバーセキュリティ」、オフィス・工場のファシリティの不正アクセスを予防する「物理セキュリティ」を重点施策として取り組んでいる。また、グローバルなデータ流通が進展することから、個人情報保護の強化が図られており、プライバシーマークを取得するとともに、2018 年 5 月 25 日より施行された EU 一般データ保護規則（General Data Protection Regulation; GDPR）の個人情報の域外移転規制への対応として、個人データ処理

者のための拘束的企業準則（Binding Corporate Rules for Processors：BCR-P）をオランダのデータ保護委員会に承認申請をしている[4]。

③金融機関の「みずほファイナンシャルグループ(FG)」【図3】

日本の大手金融機関の一つである「みずほファイナンシャルグループ」のガバナンスは、「CSR（企業の社会的責任)」の中に位置付けている。さらに、ガバナンスの中には、「コーポレートガバナンス」「コンプライアンス」「リスク管理」「事業継続管理」の管理・統制機能が掲げられている。併せて、経営体制の中のおいても、「コーポレートガバナンス」と「IT戦略」を掲げている。該社は金融機関であることから、リスク管理での総合リスクとして、①信用リスク、②市場リスク・流動性リスク、③オペレーショナルリスクを掲げるとともに、さらに、オペレーショナルリスクを細分化し、システムリスク、事務リスク、法務リスク、人的リスク、有形資産リスク、規制・制度変更リスク、レピュテーショナルリスクを掲げて、より厳格なリスク管理がなされている。これらのリスク管理は、決して金融機関のみのリスク管理の内容ではなく、一般企業においても求められるリスク管理の内容であるが、厳格なリスク管理を掲げているのは、金融機関としての社会的責任の表れと言える。

また、該社は、日本を代表する、グローバルで開かれた金融総合グループとしての社会的責任と公共的使命としての重みを常に認識し、「法令・諸規則を遵守し、社会的規範に悖ることのない誠実かつ公正な企業活動を実践すること」をコンプライアンスと考えている。コンプライアンスの徹底を、経営の基本原則として位置付けている。

経営体制の中にIT戦略を掲げており、さらに、IT戦略の中にITガバナンスの強化、ITサイバーセキュリティ及びIT次期システムの取り組みを掲げている（図3)。これらの項目は、まさしく、ITガバナンスと情報セキュリティガバナンスに関するものであり、如何に重要な経営課題として捉えているかが伺える[5]。

1．2　事例からみるガバナンスの考察

(1) 経営理念による管理統制フレームワークの違い

ガバナンスの管理統制フレームワークには、共通的な項目として、コーポレートガバナンスとコンプライアンス、リスクマネジメント（リスク管理）が挙げられるが、これら以外の項目は、経営理念や方針により異なっており、以下のことが言える。

①ガバナンスは、経営理念のもとで、持続的な成長、社会の発展に貢献、企業価値の向上の実現をめざして取り組むこととしている。そして、会計上の利益のみならず、CSRや環境問題への対応、地域（地元）への貢献度、高齢化問題など様々な取り組みにおいて、ステークホルダーから社会的評価を受けることも重要な企業価値の一つとしている。

②企業は、ガバナンスをCSRやサステナビリティの中に掲げている、これは、企業が、永続的に生き、持続的に発展するためには、経済活動のみならず、企業と社会がともに成長し、社会貢献、地球環境問題に取り組み、法定遵守することや企業倫理を遵守するなど、社会的責任の果すことであるとしている。これをCSR経営、サステナビリティ経営として前面に打ち出している。

③業種によっても、ガバナンスの中での管理・統制項目は異なっている。これは、業種により、ステークホルダーに示すべき管理・統制の考え方が異なっているからと言える。ITや情報通信の企業では、コーポレートガバナンス、コンプライアンス、リスクマネジメントの他に、情報管理（個人情報・知的財産保護、情報セキュリティ等を含む)、内部統制などが掲げられており、これらの項目は、企業活動（行動指針）と密接に関連していると言える。

④事例企業の中では、ITガバナンスや情報セキュリティガバナンスを、ガバナンスやコーポレー

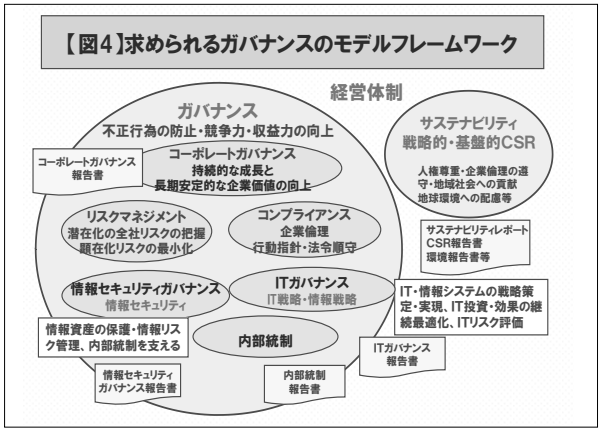
トガバンスの項目として掲げている企業はない。富士通は情報セキュリティガバナンスを情報セキュリティの基本方針の中で記載されており、みずほファイナンシャルグループは、ITガバナンスをIT戦略の一項目として掲げている。

(2) 多様化するガバナンスの考え方

情報システムが高度化し多様な不祥事が続く中、企業のガバナンスの考え方や仕組みは、少しずつ変化し進化している。また、ガバナンスは、コーポレートガバナンスと同義に使われることが一般的となり、リスクガバナンス、ITガバナンス、情報セキュリティガバナンス等の言葉が使われるようになってきた。ガバナンスは、一般的には、経営方針や理念等と同じ位置付けのように考えられがちであるが、実際にはそのような位置付になっていない。

一方、近年、ITガバンスや情報セキュリティガバナンスは、情報戦略や情報セキュリティの中に位置付けられるようになってきており、経済産業省が示すコーポレートガバンスの中でのITガバナンス及び情報セキュリティガバナンスの位置付けと異なっている[6]。概して言えることは、ガバナンスの下で共通して置かれている管理・統制項目は、多様化しており、その結果、ガバナンスは、コーポレートガバナンス、コンプライアンス、リスクマネジメント（リスク管理）に加えて、IT戦略、情報管理（個人情報・無形資産の保護）、情報セキュリティ、事業継続管理、内部統制を包含した統治の仕組みとなっている。そして、ガバナンスは、「CSR・環境・社会貢献」や「CSR」、「経営方針」などの中に位置付けられており、ステークホルダーや社会に分かりやすい言葉を使っている。

図4は、事例を参考にして筆者が考える「求められるガバナンスのモデルフレームワーク」である。ITが企業の中で戦略上、重要な役割を果たしているというならば、ITガバナンス及び情報セキュリティガバナンスは前面に押し上げて掲げるべきである。ITガバナンスの基で、情報システム戦略が立案・開発推進され、情報セキュリティガバナンスの基で情報セキュリティが実行されるのである。そして、企業がITマネジメントや情報セキュリティマネジメントを推進する上で、経営陣から見た行動指針やそのための必要な仕組みを明確化することが重要なのである。



3. 情報システムのガバナンスの位置付け

3.1 情報システムのガバナンスの定義とフレームワーク

情報システムのガバナンスの中核となるのが「ITガバナンス」と「情報セキュリティガバナンス」である。ITガバナンスの定義は諸団体により異なり、経済産業省のITガバナンスの定義は、「経営陣がステークホルダーのニーズに基づき、組織の価値を高めるために実践する行動であり、情報システムのあるべき姿を示す情報システム戦略の策定及び実現に必要となる組織能力とその仕組み」である[2]。また、日本監査役協会 ITガバナンス委員会は、「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。」としている[7]。さらに、情報システムコントロール協会（ISACA）とIT Governance Institute は、「ITガバナンスは取締役会および経営陣の責任である。それは企業ガバナンスの不可欠な部分で、リーダーシップおよび組織的な構造、および組織のITがその組織の戦略および目的を保持し拡張することを保証するプロセスから成る」としている[8]。三者の定義のポイントは、経済産業省は「組織能力と仕組み」を言い、日本監査役協会は「IT利活用とリスク対処の仕組み」を言い、ISCAは「プロセス」を主張している。

一方、経済産業省の情報セキュリティガバナンスの定義は、「社会的責任にも配慮したコーポレートガバナンスと、それを支えるメカニズムである内部統制の仕組みを、情報セキュリティの観点から企業内に構築・運用すること」であるとしており、情報セキュリティガバナンスの対象は、ITのみならず、組織の「情報資産」であり、その目的は企業価値を高めるIT及び情報システムの戦略的活用とその情報資産の保護のセキュリティ確保である。情報システムのガバナンスは、情報システム部門に閉じた課題ではなく、企業全体の経営課題であるとしている[6]。

そこで、重要となるのが、ITガバナンスや情報セキュリティガバナンスの位置付けと推進体制である。そして、実務上は多くの社員が両方の業務に携わることになり、フレームワークは整合性のとれたものでなければならない。また、経済産業省が推進する情報セキュリティガバナンスのフレームワークは、ITガバナンスの国際標準である「ISO/IEC 38500:2008(Corporate Governance of Information Technology)」[注2]を参照している。このことから、筆者は、経営レベルのITガバナンスと情報セキュリティガバナンスは統合した組織で所管し、推進されるべきであると主張している。

3．2 ITガバナンスと情報セキュリティガバナンスの位置付けの問題

経済産業省は、「ITガバナンス」と「情報セキュリティガバナンス」は、コーポレートガバナンスの一環として位置付けている。また、ITガバナンスと情報セキュリティガバナンスを一方が他方を包含する関係ではなく、一部を重複する明確に異なる関係になるとしている[6]。この関係は概念の位置付けと言えるが、前章の事例では、ITガバナンス及び情報セキュリティガバナンスをコーポレートガバナンスの中に位置付けていない。

コーポレートガバナンスは、一般的には、①「企業の不正行為の防止」と②「競争力・収益力の向上を総合的にとらえ、長期的な企業価値の増大に向けた企業経営の仕組み」であるとしている。近年、不祥事が多発するなかで、企業経営で注目すべきこととして、2015年6月から上場企業に導入されたJPX(東京証券取引所）の「コーポレートガバナンス・コード」がある。本コードでは、「会社が、株主をはじめ顧客・従業員・地域社会等の立場を踏まえた上で、透明・公正且つ迅速・果断な意思決定を行うための仕組みを意味する。」としており、コーポレートガバナンス・コードの基本原則は、①株主の権利・平等性の確保、②株主以外のステークホルダーとの適切な協働、③適切な情報開示と透明性の確保、④取締役会等の責務、⑤株主との対話の5つである[8]。

本コードであっても、ITガバナンス及び情報セキュリティガバナンスを、基本原則のなかで位置付けしていない。もちろん、企業が本コードを適用する義務はない。独自のコーポレートガバナンスの基準を制定することは可能であるが、その場合にはステークホルダーへの説明責任を果たすことが必要である。

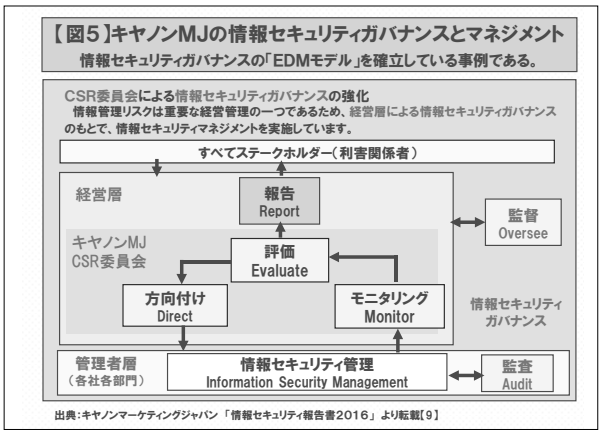
3．3 国際標準の情報セキュリティガバナンスを位置付けた企業

ITガバナンスの国際標準である「ISO/IEC 38500」を基に、ITガバナンス及び情報セキュリティガバナンスを確立している企業は少ない。しかし、通信企業のNTTと先進的な「イメージングとIT」のソリューションカンパニーであるキヤノンMJグループは、情報セキュリティマネジメント体制を構築し、情報セキュリティガバナンスを確立している企業である。図5は、キヤノンMJグループの情報ガバナンスとマネジメント体制である。

該社では、「CSR・環境」の中に、「情報セキュリティ」を位置付けている。また、「情報セキュリティガバナンスとマネジメント」なかで、『「セキュアな社会の実現」に寄与するために、経営層による「情報セキュリティガバナンス」に基づき、「情報セキュリティマネジメント」を推進し、情報セキュリティ成熟度の向上に取り組んでいます。』と記載している。また、情報セキュリティの取り組みは、コンプライアンスや環境対応、事業継続、品質管理などの社会要請への対応と密接に関連するとしている[10]。

情報セキュリティガバナンスの所管は、「キヤノンMJCSR委員会」とし、その中で経営陣が情報セキュリティガバナンスを取り組んでいる。そして、この委員会で、情報セキュリティ方針や戦略などの決定「方向付け（Direct)」を行い、定期的に経営環境やリスクの変化、目標の達成状況などを「確認（Monitor)」し、「評価（Evaluate)」するサイクルを回している。その上で、これらの一連のガバナンスと、そのもとで取り組まれてい

る情報セキュリティマネジメントの状況は、「情報セキュリティ報告書」を通じて、社内外のステークホルダーに「報告（Report)」されている【図5】。



4．情報システムのガバナンスの確立と監査

4．1　情報システムの構築構造と情報システムのガバナンス

情報システムなしには経営は成り立たない。そこで、情報システムを活用して経営戦略を実現するために、「IT ガバナンス」を確立し、推進する組織能力とその仕組みが必要となる。一方、その情報システムを安全に信頼して活用できるように、「情報セキュリティガバナンス」を確立し推進する組織能力とその仕組みが重要となる。情報システムの構築構造は、まず、経営戦略や情報戦略の「経営」から、情報の有効活用や管理の「情報」になり、そして「情報システム」が構築される。しかし、情報システムが構築されると、情報が作成されて、活用され、情報を経営戦略の実現に活用することで競争優位が展開できる。この情報システムから経営戦略の実現への流れを、IT 活用の側面から「IT ガバナンス」の確立が求められ、情報資産の保護の側面から「情報セキュリティガバナンス」が確立され、推進することになる。この「経営 - 情報 - 情報システムの構築」の方向付けの流れと「情報作成 - 活用 - 経営戦略の実現」の流れが、スムースになるように情報システムのガバナンスの確立が求めれる。

4．2　情報システムのガバナンス確立の組織体制

IT ガバナンスは、経営陣がステークホルダーのニーズに基づき、組織の価値を高めるために実践する行動であり、情報システムのあるべき姿を示す「情報システムの戦略策定と実現」である。一方、情報セキュリティガバナンスを確立するには、経営陣は、情報資産に係る機密性、完全性、可用性の観点からリスクを見直す必要がある。そのためには、情報資産に係るリスク管理を狙いとして、情報セキュリティに関わる意識、取り組み及びそれに基づく業務活動を組織内に徹底させる仕組みを作る必要がある。

IT ガバナンス、情報セキュリティガバナンスともに、経営戦略・情報戦略から落とし込まれるものであり、その推進体制は、経営陣から選任された CIO や CISO 等とともに経営戦略から情報戦略への立案を推進する経営企画、情報企画部門等及び情報システムを開発する主要メンバーから構成された「情報システムのガバナンス委員会（仮称）」等が現実的である。実務的には、多くの社員が両方の業務を携わることになり、IT ガバナンスと情報セキュリティガバナンスとともに、「情報システムのガバナンス委員会（仮称）」が、その確立の責務を負うことになる。中小企業の場合には、経営者が委員長となって、構成することも考えられる。事例であげたキヤノン MJ グループの「CSR 委員会」の所管組織が「情報システムのガバナンス委員会（仮称）」と同じ位置付けと言える。

4．3　情報システムのガバナンスの監査の課題と実施

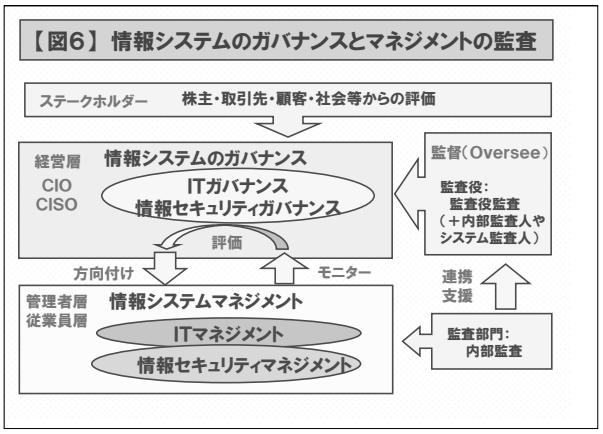
これまで IT ガバナンスが適切に実現されたのかどうか、あるいは、実現を支援する監査（システム監査を含めて）が実施されてきたのか、その事例はほとんど見受けられない。一般社団法人日本内部監査協会が 2019 年 2 月に発行した「監査白書　2017 年」によると、監査役による IT ガバナンスを対象とした監査は実施されていない。しかし、同白書の「情報システム監査」において、監査対象に「情報システム戦略の全体的方針と整合性」があげられており、情報システム監査を実施している企業の中で、55.8% の企業が、この監査対象の監査を実施している。「情報システム戦略の全体的方針と整合性」は、新たなシステム管理基準が最初に掲げている「情報システム戦略の方針及び目標選定」の中で、「経営陣は、経営戦略の方針に基づいて情報システム戦略・目標設定及び情報システム化基本計画を策定し、適宜に見直しを行っていること。」に該当し、このことから IT ガバナンスの監査が実施されていないとは言えない。ただし、この監査は内部監査人よる IT ガバナンス関連項目の監査である。

また、監査対象に情報セキュリティ（ウイルス対策・個人情報保護等）管理やシステムの企画・設計・開発管理が実施されており、これらの内部監査において、経営陣が評価し、方向付け・モニタリングされているならば、IT ガバナンスの情報セキュリティ（IT ガバナンスがカバーしている範囲の情報セキュリティを言う）が確立できていることになる。ただし、その実現の適切性等の評価や保証は監査の実施によって担保されるのであるが、それは監査役による監査でもなく、保証型の監査でもない。

（1）情報システムのガバナンスの監査の実施

情報システムのガバナンスの監査は、原則的には監査役により実施され、指摘事項があれば改善が求められる。また、監査の結果は、外部のステークホルダーへの報告と評価を受けることになる。このことから、監査とともに外部評価による指摘・改善が発生することから「監督（Oversee）」となる[図6]。また、前述の事例「図５　キヤノン MJ の情報セキュリティガバナンスとマネジメント」の中で監査と監督の位置付けが示されている。

そこで、現実的な問題として、専門性の高い情報システムのガバナンスの監査・監督は、監査役のみでできるのか、また、監査の対象や監査のポイントはどこになるのかと言った問題が起こってくる。筆者は、情報システムのガバナンスの監査・監督は以下のように考える。



①監査を実施する主体は監査役であるが、情報システムマネジメント及び情報セキュリティマネジメントの監査を実施したシステム監査人や内部監査人の支援や連携体制による監査となる。そこで、監査役は監査責任者となる。この体制をとることで、監査役としての監査責任は保たれ、専門性の高い有効な監査が実施できる。

②監査対象組織は「情報システムのガバナンス委員会（仮称）」とし、委員会組織の取組み内容や役員会等での報告を対象に、経営者が EDM（評価・方向付け・モニタリング）モデルによる取り組むべき事項、内容についても監査・監督を実施する。

③監査のポイントは、経営陣に代わる「情報システムのガバナンス委員会（仮称）」が、IT ガバナンスを策定・確立し、IT ガバナンスに基づいた情報システムが戦略的で効果的な情報システムを構築しているか、IT 投資は適切で投資効果は有効であるか、また、情報セキュリティガバナンスに基づいた情報セキュリティは有効に機能しているか、情報セキュリティ投資は適切で投資効果は有効であるか、等が挙げられる。さらに、ステークホルダーへの報告と評価を「情報システムのガバナンス委員会（仮称）」で、充分に討議し改善に繋げているか、と言ったことは、経営陣の視点で E（評価）、D(方向付け)、M（モニター）されているかがポイントとなる。これらの監査のポイントは、あくまで「情報システムのガバナンス委員会（仮称）」が経営陣に代わって実行されるもので、最終的な責務は経営陣自身であることが意識の中になければならない、その意識付けは監査役の責務である。

5．おわりに

筆者は、企業のなかでコンピュータ犯罪や事故でのセキュリティ対策やシステム監査の研究をしてきた。しかし、近年、企業で不祥事が発生し、そのたびにガバナンスの問題が指摘されるようになった。そこで、ガバナンスの確立に、システム監査やセキュリティ監査がどのように関わることができるのか、高い視点（俯瞰的な視点）で見る必要がある。ガバナンスの確立が経営陣の行動に関わるからである。いみじくも、昨年に「システム管理基」が改訂・公表され、経営陣による IT ガバナンスの確立の重要性を強調した。

本稿は、企業のガバナンスの考え方を知る手がかりとして、まず、主要企業のガバナンスについて調査し、その結果、企業組織全体からのガバナンスの位置付け及びガバナンスの内容として掲げられた管理統制フレームワークを作成し、その位置付けを明らかにすることができた。

一方、情報システムが高度化することで、情報システムのガバナンスの確立に貢献するシステム監査が非常に重要となってきた。

しかし、情報システムのガバナンスの確立は、第一義的には、経営陣により方向付けされるものであり、監査は、監査役が実施する業務監査の一貫として位置付けられており、システム監査が貢献するには、より実践的なアプローチが必要である。その具体的な手法や手続きは、今後の研究課題と考えている。

【注】

【注 1】文献や企業のホームページ等では、コーポレートガバナンスとコーポレート・ガバナンスの用語が使われている。本稿では、コーポレートガバナンスに統一した。

【注 2】ISO/IEC38500（IT ガバナンス）
本規格は、ISO（国際標準化機構）と IEC（国際電気標準会議）の総会で承認された「SC40 専門委員会（IT サービスマネジメントと IT ガバナンス）」において、IT ガバナンスおよび IT サービス管理に関する標準、ツール、フレームワークである。組織のガバナンスを実施する経営者層に対し、①評価（Evaluate）②方向付け（Direct）③モニター（Monitor）の 3 つを実践することが経営者としての役割、と定義している。情報システムマネジメントしての PDCA サイクルによるマネジメントモデルの上位に、ガバナンスモデルとして EDM モデルが位置付けられる。なお、日本では 2015 年 7 月に「JIS Q 38500:2015　情報技術　IT ガバナンス」のみが JIS 化されている。

【参考・引用文献】

【1】「ガバナンス」 実用日本語辞典　https://www.weblio.jp/content/ （2019 年 4 月 9 日）

【2】経済産業省（2018）「システム管理基準」平成 30 年 4 月 20 日

【3】「ガバナンス」トヨタ　ホームパージ （2018 年 11 月 13 日）
https://global.toyota/jp/sustainability/esg/

【4】「社会・環境分野の取り組み」富士通ホームページ　https://www.fujitsu.com/jp/about/csr/（2019. 年 4 月 9 日）

【5】「CSR（企業の社会的責任）」「経営体制」
みずほファイナンシャルグループ　ホームページ（2018 年 11 月 13 日）
https://www.mizuho-fg.co.jp/company/structure/index.html

【6】経済産業省「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報告書」 平成 17 年 3 月

【7】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　平成 23 年 8 月 25 日

【8】JPX（株式会社東京証券取引所）「コーポレートガバナンス・コード」 2018 年 6 月 1 日

【9】ISACA IT ガバナンス導入ガイド 第 2 版
IT ガバナンス /IT-Governance-Implementation-Guide_res_Jpn_1211.pd

【10】経済産業省 「情報セキュリティガバナンスの導入ガイダンス」平成 21 年 6 月

【11】「キヤノン情報セキュリティガバナンスとマネジメント」「情報セキュリティ報告書」
https://cweb.canon.jp/csr/security-report/pdf/security-all2017.pdf （2018 年 3 月 16 日）