特集 最新ガバナンス事情

情報セキュリティガバナンスの重要性

工学院大学 情報学部
大木　榮二郎

1 情報化の進展と組織のガバナンス

1-1　リスクの変質

情報化の進展は、企業や団体などの経営組織に様々な影響をもたらしている。関係者間の情報共有が進み、業務が効率化し、行政サービスが向上するなどのプラスの効果に加え、一方で情報セキュリティの確保に代表される組織体のリスク対応に質的な変化を求める影響も見逃せない。

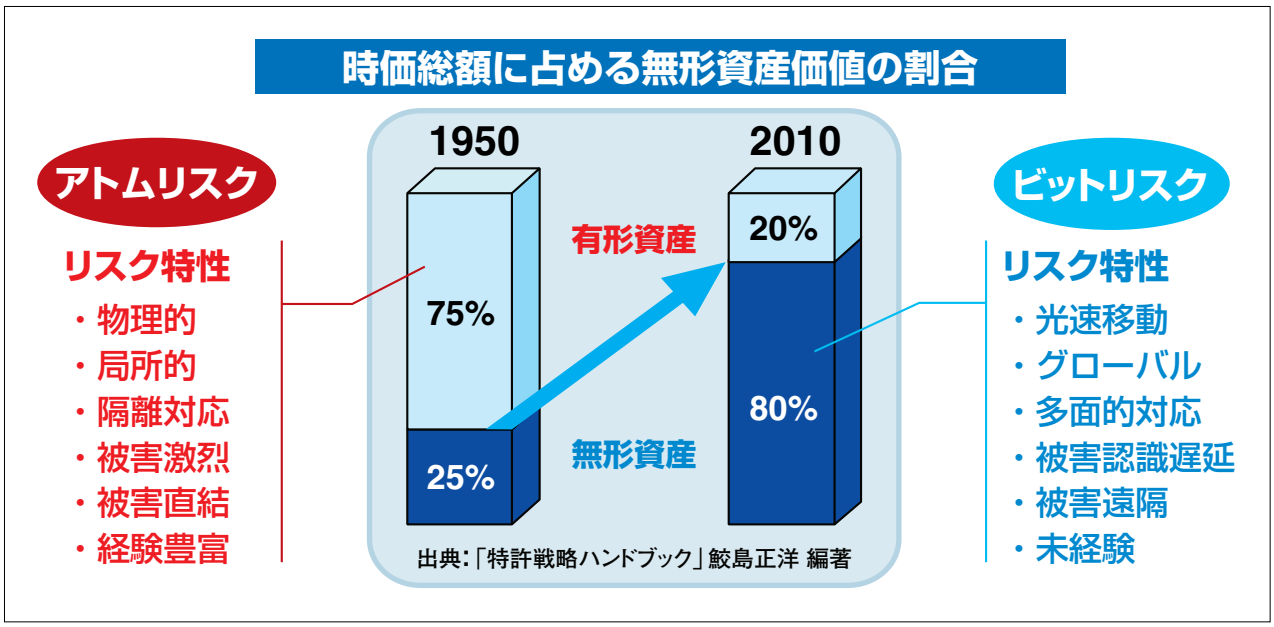
このようにリスク対応に質的変化が求められる根本原因は、リスクそのものの変質にあると思われる。

組織体の経営にとってのリスク管理は、特に目新しいものではなく、これまでも経営者の主たる意思決定の中心にあった課題である。しかし経営者が対応すべきリスクの特性が、情報社会を迎えてかなり変質してきていると見る必要があるのだ。

企業を例にとって、情報化進展の前後で直面するリスクがどのように変質したかを見ると、よくわかる。**図1**は、米国の例であるが、1950年と2010年の全上場企業の企業価値（株式時価総額で評価）を有形資産と無形資産との構成比で示している。この60年間に劇的な構成変化が見て取れるが、これが情報化の大きな成果と言えよう。

組織経営者の大きな任務がこの資産に対するリスクだとすると、これまでの有形資産に関するリ

図1　企業価値の構成変化と経営リスク



スクマネジメントから、無形資産のリスクマネジメントへ大きく舵を切らなければならないことが分かる。これ以降、有形資産に係るリスクをアトムリスク、無形資産はその多くがデジタル化されていることからそれに係るリスクをビットリスクと名付けて、その本質的な違いを探ってみよう。

アトムリスクは、工業化社会の主役であった土地、建物、工場設備、製品などのモノに係るリスクで、危険物、貴重物に関するリスクが主体であるから、ひとたびことが起きると被害が激烈で膨大な損失に直結する。そのための対策は、危険物や貴重物を物理的に隔離し保護策を講じて厳重に管理するなど、物理的、局所的かつ直截的な管理策が有効であり、経営者にも理解しやすく管理経験も豊富であると言える。

これに対し、ビットリスクはかなり異なる特性を持つ。ビットはネットワークを通じて光速で世界中を駆け巡る。必然的にグローバルな広がりを本質的に持ち、物理的、局所的な対策だけでは対応できない多面的な対策を必要とする。ひとたびことが起きてもすぐに激烈な被害が発生するわけではないが気がつかないうちにじわじわと被害が拡大する、事故の原因と被害とが時間的にも空間的にも離れているが、全体像が明らかになるとその組織に対する社会的な信頼を失墜し存在意義まで疑われることになりかねない重大性も秘めている。

つまり、ビットリスクへの対応は、アトムリスクに比べると極めて厄介な性質を持ち、経営者にとっては経験が少なく、難しいリスク対応が求められることになる。

対策に手を抜いたところで、すぐに問題が明らかになるわけではないが、ボディーブローのように組織体力にじわじわと影響を与え、気がつくと大事に至っているという性格のリスクに直面していると考えなければならない。

1-2　情報リスクのマネジメントを主眼とした組織ガバナンス

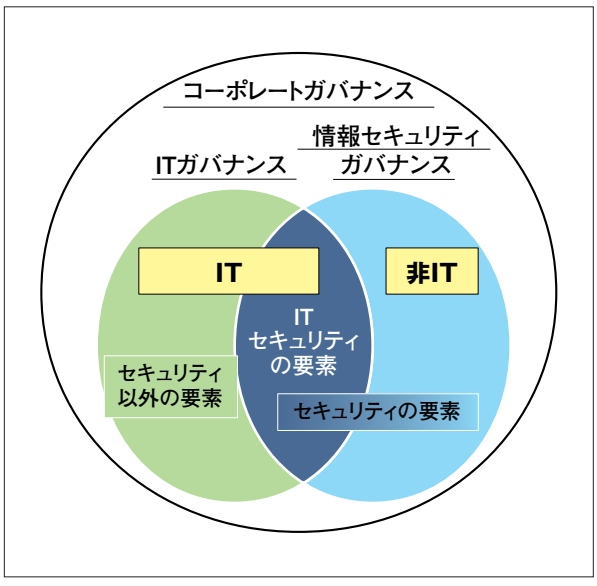
このビットリスクへの対応は、これまでITに係るリスクとしてとらえられてきた。企業では、コーポレートガバナンスの構成要素として、ITガバナンスが提唱されて久しい。

しかし、ビットリスクの全体がITガバナンスでカバーされるわけではない。ITガバナンスはテクノロジーに係るリスクを対象とするが、情報セキュリティに係るリスクは、IT以外の部分にも存在することになり、本質的に組織が活用する情報に係るリスク全体をカバーするには、別の見方が必要になる。

行政組織においては、住民に係る重要情報を必然的にほとんどの業務において利用することから、ITという技術に係るリスクの管理という側面よりも、住民情報のセキュリティというリスク管理の側面のほうがより本質的に重要な意味を持ってくると考えられる。

さらに、テクノロジーに係るリスクの側面は、例えば共同センターの利用、あるいは今後クラウドの利用などにより、リスク管理の多くを行政組織の外に移転することも考えられるが、業務に直結する情報のセキュリティに係るリスクの対応は行政組織が主体的に行わなければならない。このような意味で、行政組織においても、組織のガバナンスの要素として、情報セキュリティガバナンスは欠かすことのできないものとなっていると考える必要がある。**（図2参照）**

図2　ITガバナンスと情報セキュリティガバナンス



2 情報セキュリティガバナンスとは

2-1　情報セキュリティガバナンスの枠組み

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要素として、企業を想定して検討されたものであるが、行政組織にもその考え方は大いに役立つものである。

組織の情報セキュリティ対策を歴史的にみれば、最初は例えば暗号など技術的な対策の検討から始まったが、技術だけでは守れず人の対策が必要となり、さらに、組織的な対応へと広がってきた。

これらの対策の効果を一定水準に向上し維持するために、PDCAのマネジメントプロセスが導入され、情報セキュリティマネジメントとして定着しつつある。

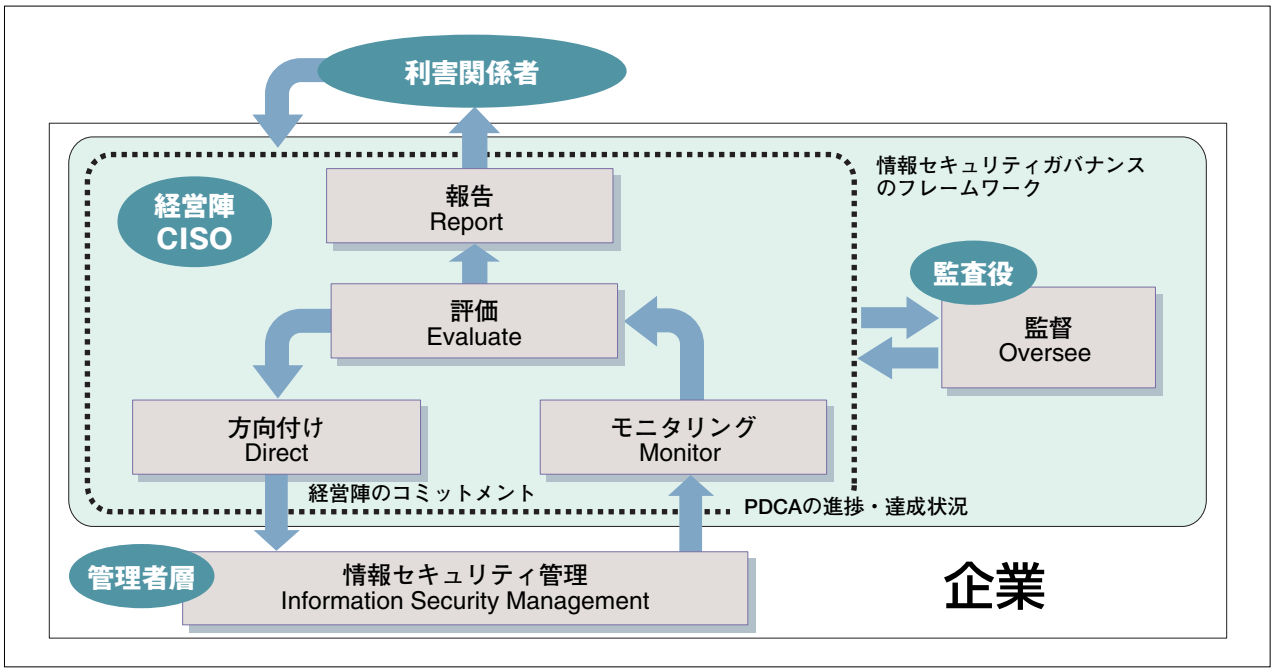
これまでのこのような対策の発展は大いに評価できるが、しかし、このようなセキュリティマネジメントを導入した組織においても、そこで働く人の意見に耳を傾けると、さまざまな問題指摘が聞こえてくる。

例えば、情報セキュリティマネジメントに対して組織の経営トップの理解が得られにくい、あるいは現場には様々な対策を押しつけられて「やらされ感」が蔓延している、さらには、なぜここまでやらなければならないのかわからないなど反発に近い声などもある。

これまでの情報セキュリティマネジメントは、ほとんどのケースで管理者層を中心に進められてきたが、そこにどこまで経営層が関与しているのかが大きなポイントである。各種のアンケートによれば、経営層の多くが、「情報セキュリティ対策をどこまで行えばよいのか分からない」と回答しているケースが多い中で、経営層が消極的にしか関与していないまま、管理者層による情報セキュリティマネジメントが推し進められた結果ではないかと思われるのだ。

つまり、経営層と管理者層との間の意思疎通ができているのかが大きなポイントとなる。この解決のためには、経営層がビットリスクについての理解を深め、情報セキュリティの取り組みを組織経営の主要なリスク対応の一つとして取り組むことが求められる。そのために、経営者が何をしなければならないかを明らかにしたのが、**図3**に示す情報セキュリティガバナンスフレームワークである[注1]。

図3　情報セキュリティガバナンスのフレームワーク



経営層がビットリスクを理解し、組織に必要な情報リスクマネジメントの方針を明確にして、「方向付け（Direct）」として管理者層の情報セキュリティマネジメントに示す。「何のためにどこまでやるか」を明確にすることが重要である。それを受けて、管理者層と従業者層で情報セキュリティマネジメントに取り組む。その過程を経営層は「モニタリング（Monitor）」することでその効果を確認し、「評価（Evaluate）」にて組織としての対応全体を評価し、方向付けに反映する、あるいは組織外の利害関係者に「報告（Report）」することなどが、経営層の主な活動と位置付けられる。「監督（Oversee）」は、企業と行政組織とではやり方がかなり異なるであろうが、意味付けとしては経営層のこのような情報リスクへの的確な対応を監督するという役割を果たす。

2-2　行政組織において経営層が果たすべき役割

情報セキュリティマネジメントが十分に効果を発揮できない原因の多くは、経営層と管理者層との間のコミュニケーションにあり、経営層が果たすべき役割は極めて大きい。しかも、経営層は組織が直面しているすべてのリスクに対応する責任を追っている立場であるが、ビットリスクの特徴を正確に理解し、情報セキュリティについての的確な方向付け（Direct）をするのはそうたやすいことではない。そこで、多くの組織では経営層のなかでビットリスクに専門的に対応する役員（CISO : Chief Information Security Officer、最高情報セキュリティ責任者）を配置し始めている。

CISOの役割は、組織のリスク全般の管理方針から、ビットリスクの管理方針を明確にして、情報セキュリティマネジメントの目的や目標に展開して管理者層に明示すること（Direct）と、それが管理者層従業者層でどのように効果をあげているかモニタリングする（Monitor）ことである。そして、これらを踏まえて、経営層において行う評価（Evaluate）に参画し、ビットリスク固有の特性を踏まえた評価を全般的なリスクの中に位置付けて、さらにビットリスク対応力を維持向上していくことに責任を持つ。つまり、経営層と管理者層との間のギャップを埋める働きが求められている。

このギャップをうまく埋めることで、「なんでこんな対策まで押しつけられるのか」という現場の反発を、「行政サービスではここまでやらなければ」というような意識に変化させることもできるし、経営層も自信を持ってもう少し頑張らなければならないと思えるようになるはずである。

組織全体が主体的にビットリスクの対応に取り組むようになるかどうかは、まさしく経営層の取り組みにかかっているのである。

2-3　組織内のリスクコミュニケーション

情報セキュリティガバナンスフレームワークで示した方向付け（Direct）とモニタリング（Monitor）は、言い換えれば経営層と管理者層との間のリスクコミュニケーションである。さらに、管理者層と従業者層で行われる情報セキュリティマネジメントにおいても、計画（Plan）、実施（Do）、評価（Check）、改善（Act）のサイクルを通じて、管理者層と現場の間でさまざまにリスクコミュニケーションが行われることになる。その際、方向付け（Direct）や計画（Plan）のコミュニケーションは、目的・目標を明確にし、何のためにどこまでやらなければならないかが示されれば、それを現場にブレークダウンすることで比較的容易に円滑なコミュニケーションがはかられるであろう。

しかし、その成果をみる評価（Check）あるいはモニタリング（Monitor）において、正確なリスク情報を収集し伝達するには、もうひと工夫必要である。

各種の対策が実施されている現場の実際のリスクがどの程度になっているかが情報セキュリティ監査で確認され、監査報告書として報告されることが、このリスクコミュニケーションの要点となる。そのためには、情報セキュリティの内部監査を実施する手順や体制の確立とともに監査要員の育成などに取り組まなければならない。

同時に、経営層のみならず管理者層や従業者層

においても、ビットリスクやリスクコミュニケーションについて適切に理解し、リスクコミュニケーションに参画することが求められる。

3 情報セキュリティ報告書の紹介

3-1 組織外関係者とのリスクコミュニケーションの重要性

組織内のコミュニケーションに加えて、組織の外にいる関係者とのリスクコミュニケーションも極めて重要である。行政組織においては、組織外関係者は、行政サービスを提供する上で業務を委託する先となる事業者が一つの関係者であり、もうひとつ最も大事な関係者が行政サービスを提供する先、つまり地域住民ということになる。前者とのリスクコミュニケーションは前章のリスクコミュニケーションに準ずる側面もあり、ここでは住民とのリスクコミュニケーションを取り上げることにする。

行政組織は、住民の個人情報をいわば強制的に収集し、行政サービスに利用している。また、そこで発生する費用はすべて税金で賄われていることから、行政の過程における情報セキュリティの確保について、行政組織の長は説明責任を負っていることは間違いない。この説明責任を果たす有力な道具が情報セキュリティ報告書である。

政府の第2次情報セキュリティ基本計画には、情報セキュリティ報告書について次のように記述されている[注2]。

「各政府機関においては、行政に対する国民の信頼の確保に向けて情報セキュリティ対策に係る説明責任を明らかにする観点から、それぞれの情報システムの現状を把握した上で、情報セキュリティに対する考え方、情報セキュリティ対策に係る目標や計画及びその実績と評価など、それぞれの政府機関においてPDCAサイクルが有効に機能しているかどうかを 数値指標などの客観的指標を積極的に活用して記述した『情報セキュリティに係る年次報告書』（情報セキュリティ報告書）を作成する。作成した情報セキュリティ報告書は、最高情報セキュリティ責任者が、情報セキュリティ政策会議の下に設置されている情報セキュリティ対策推進会議等の場において報告し、公表する。」

つまり、情報セキュリティ報告書は行政機関から国民に向けてのリスクコミュニケーションの有力な手段であり、CISOが中心となってその作成に取り組み公表することで関係者に示されることになる。これまではもっぱら組織内のことと受け止められていた情報セキュリティの取り組みについて、住民に説明し理解を得ることが必要となっている。

3-2 情報セキュリティ報告書の機能

情報セキュリティ報告書は、もともとは企業の情報セキュリティガバナンスの一環として検討されてきたものである。つまり、先ほどの情報セキュリティガバナンスフレームワークの「報告（Report）」の手段として構想されたもの[注3]であり、当初は企業を想定してその内容が検討されたが、その後、企業のみならず、行政組織を含めた様々な組織における情報セキュリティについての説明責任を果たす道具として注目を集めている。

この報告書には、**図4**に示すごとく7つの記載項目が設定されている。今後すべての行政組織が、このような年次報告を公開するとの前提で、内部の情報セキュリティ監査などによる正確なリスク情報の把握を通じて、情報セキュリティガバナンスの確立とリスクコミュニケーションの充実に取り組んでいただきたい。

4 情報セキュリティガバナンスに求められる人材

このような情報セキュリティガバナンスを確立するには、それを支える人材の育成が欠かせない。

最も重要な役割を果たすCISOの育成がまずは急

務である。首長など、行政組織のトップがビットリスクの特性を理解することももちろん必要であるが、リスク全般の管理方針から当該組織固有の具体的な情報セキュリティ目的・目標に展開して方向付けをするという作業は、広範な知識と経験を必要とする。CISOの明確な職務規定を定めて育成していくことが重要である。短期的に、このような人材を行政組織内で見つけるのが難しい場合は、補佐官制度などで補うことも有効であろう。

そのうえで、このCISOの方向付けを受けて情報セキュリティマネジメントを実践する管理者の育成、IT部門でコンピュータやネットワークの技術的専門的なセキュリティ対策を担当する技術者、業務部門においてリスクを分析評価し、業務プロセスにセキュリティ対策を組み込むスタッフ、あるいは組織全体のセキュリティ研修を企画し実施するスタッフなどの育成も求められる。さらに、情報セキュリティの内部監査を行う情報セキュリティ監査人の育成も重要である。

行政組織の規模によっては、これらの人材を外部に依存することもあり得るが、行政組織が住民に対する説明責任を効果的に果たしていくには、情報セキュリティガバナンスの骨格を支える人材がすべて外部リソースというわけにはいかない。情報の的確な管理能力は行政機関の最も大事な中核能力の一つに違いないからである。

的確な人材育成を計画することで、情報セキュリティガバナンスの確立を支える人材が早期に育ってくることを期待したい。

【注】

1.経済産業省「情報セキュリティガバナンス導入ガイダンス」参照
http://www.meti.go.jp/press/20090630007/20090630007-2.pdf

2.内閣官房情報セキュリティセンター「第2次情報セキュリティ基本計画」
http://www.nisc.go.jp/active/kihon/pdf/bpc02_ts.pdf

3.経済産業省「情報セキュリティ報告書モデル」
http://www.meti.go.jp/policy/netsecurity/downloadfiles/070824securityreportmodel.pdf

図4　情報セキュリティ報告書の記載項目