情報セキュリティガバナンス導入ガイダンス

平成 21 年 6 月

経済産業省

はじめに

情報セキュリティ対策は、昨今、多くの事故が報道され、その対応が急務とされているにも関わらず、今なお多くの企業において「（企業の利益に直結しない）コスト」の位置付けであり、対策を実施することの重要性が十分に理解されていない。しかし、企業内・企業間における情報資産の効率的・効果的利活用が企業活動の成否を左右する現在、経営者は、情報資産の管理が経営戦略そのものであり、それを支えるリスク管理の一環としての情報セキュリティ対策こそバリューチェーン・サプライチェーンの高付加価値化を支える重要な要素であること、グループ統制の観点に立ち、正面から対峙しなければならない経営課題であることを改めて認識する必要がある。

加えて、経営者は、企業が保有する情報の中に、法令や契約で利用が制限されている情報が含まれ、取扱にリスクが伴うケースもあること、また、顧客等が企業に対して適法性のみならず適正性を期待していることにも配慮する必要がある。例えば、実際に情報流出やシステムダウン等の事故が発生した場合、企業が適法な範囲で事故に対処したとしても、それだけでは、顧客や取引先、従業員等を含む利害関係者から適切な評価を受けられず、一層の透明性や事業継続性の確保を求められる可能性がある。そのような状況に備え、情報セキュリティに取り組む姿勢や事故対応等の情報を適切に開示[1]し、説明責任を遂行している企業事例も見ることができる。

こうした現状を鑑み、経営陣においては、自らの経営課題の一つとして、情報資産に係る機密性、完全性、可用性の観点を取り入れて、リスク管理を捉え直すことが重要である。すなわち、様々なリスクのうち、情報資産に係るリスクの管理を狙いとして、情報セキュリティに関わる意識、取組及びそれらに基づく業務活動を組織内に徹底させるための仕組み（経営者が方針を決定し、組織内の状況をモニタリングする仕組み及び利害関係者に対する開示と利害関係者による評価の仕組み）を構築・運用する、すなわち情報セキュリティガバナンスの確立に取り組むべきである。

経済産業省では、企業における情報セキュリティ対策を、従来の対症療法的なアプローチから、企業価値を高めるための投資対象として位置付けるアプローチの重要性・優位性を示すため、平成 16 年度に「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研究会」を開催して情報セキュリティガバナンスの考え方を示した。続けて、平成 17、18 年度と、情報セキュリティガバナンス確立実現の促進ツールとして、「情報セキュリティ対策ベンチマーク」、「情報セキュリティ報告書モデル」及び「事業継続計画策定ガイドライン」を開発・公開し、これらの活用事業を推進してきた。さらに平成 19 年度からは、リスク管理の必要性を軸に、情報セキュリティガバナンスの定義を明確化するとともに、情報

[1] 情報セキュリティ対策の詳細、事故の原因等の情報は攻撃者にとっても有用な情報であることから、情報の適切な開示範囲（開示対象者、開示情報種別）について、十分な考察を行うことが必要である。

セキュリティガバナンスの確立を妨げる問題点に焦点を当て、その解決策の指針となる成果を策定してきた。

本書は、経営陣と管理者層・従業員層の間でリスクや対策についての共通認識が乏しく、全体最適化された構築・運用がなされないという問題への対処指針として、経営陣が取り組むべき行動の指針を示す。これは、企業の情報セキュリティ管理手法の国際標準 ISO/IEC 27001:2005[2]の中の「Management commitment（経営陣のコミットメント）」に係る経営陣の行動指針や必要な仕組みについて明確化したもので、ISO/IEC27001:2005 を補完する位置付けとなる。

[2] ISO(International Organization for Standardization: 国際標準化機構)及び IEC(International Electro technical Commission: 国際電気標準会議)が共同で審議・策定した国際標準「Information technology − Security techniques − Information security management systems − Requirements 情報技術 - セキュリティ技術 - 情報セキュリティマネジメントシステム- 要求事項」。2005 年発行。

目次

1. 情報セキュリティガバナンスとは何か ..... - 1 -
1.1. 定義 ..... - 1 -
1.2. 適用範囲 ..... - 1 -
1.3. 位置付け ..... - 1 -
1.3.1. コーポレートガバナンス、IT ガバナンスと情報セキュリティガバナンス - 1 -
1.3.2. 情報セキュリティマネジメントシステムと情報セキュリティガバナンス - 2 -
1.4. フレームワーク ..... - 3 -
1.4.1. 前提 ..... - 3 -
1.4.2. フレームワークの構成 ..... - 3 -
1.5. 本書の利用について ..... - 6 -
1.5.1. 本書の狙い ..... - 6 -
1.6. 本書の利用者 ..... - 7 -
2. 情報セキュリティガバナンスの効果 ..... - 8 -
2.1. 経営陣によるリスク管理の実現と情報セキュリティ活動の徹底 ..... - 8 -
2.2. 基盤整備の遂行と法令遵守の徹底 ..... - 8 -
2.3. 経営品質の向上 ..... - 9 -
2.4. 株式市場の高評価とブランド価値向上 ..... - 9 -
2.5. 事故時のネガティブな反応の抑制 ..... - 10 -
3. 方向付け ..... - 12 -
3.1. リスク管理方針の決定 ..... - 12 -
3.1.1. 企業に求められるリスク管理 ..... - 12 -
3.1.2. 企業を取り巻くリスク ..... - 12 -
3.1.3. 企業におけるリスク管理 ..... - 13 -
3.1.4. 経営陣によるリスク管理方針の決定 ..... - 13 -
3.2. リスク管理の方法論 ..... - 15 -
3.2.1. リスク管理体制 ..... - 15 -
3.2.2. リスクマネジメントモデル ..... - 16 -
3.3. 情報セキュリティ目的・目標の設定と管理策への展開 ..... - 16 -
3.3.1. CISO による目的・目標設定 ..... - 17 -
3.3.2. 管理者層による情報セキュリティ管理目的・管理策の設定 ..... - 18 -
3.4. 個別の課題 ..... - 20 -
3.4.1. 企業グループのセキュリティ ..... - 20 -
3.4.2. 危機管理モデル ..... - 22 -
4. モニタリング ..... - 25 -

4.1. モニタリングで把握する内容 - 25 -
4.1.1. 経営陣が行うモニタリング - 25 -
4.1.2. CISO が行うモニタリング - 26 -
4.1.3. 管理者が行うモニタリング - 26 -
4.2. モニタリング指標の考え方 - 27 -
4.2.1. 測定項目とモニタリング指標の決定 - 27 -
4.2.2. 測定の可視化 - 28 -
4.3. モニタリングで把握する内容と対応するモニタリング指標の例 - 30 -
4.3.1. 経営陣の場合 - 31 -
4.3.2. CISO の場合 - 31 -
4.3.3. 管理者の場合 - 33 -
5. 評価 - 35 -
5.1. 経営陣が行う評価 - 35 -
5.2. CISO が行う評価 - 36 -
6. 監督 - 37 -
6.1. 監査役監査による対応 - 37 -
6.2. 内部監査との連携 - 38 -
7. 情報セキュリティに関する報告 - 40 -
7.1. アカウンタビリティと価値創造 - 40 -
7.2. 法定開示と自発的開示 - 41 -
7.3. 情報セキュリティ開示の対象と内容 - 41 -

1. 情報セキュリティガバナンスとは何か

1.1. 定義

企業の経営陣（代表取締役、取締役、役員等)は、企業価値向上と社会的責任の遂行を目的として、経営や業務の執行に取り組む。その上で、経営陣が適法性・適正性のいずれの観点からも責任を持って取り組まなければならない活動の一つに、リスク管理がある。経営陣が対峙しなければならないリスクは多様であるが、業種・業態・保有情報等によっては、情報資産に係るリスクが重大なものとして位置付けられることがある。

つまり、経営陣においては、自らの経営課題の一つとして、情報資産に係る機密性、完全性、可用性の観点からのリスク管理を捉え直すことが重要である。すなわち、様々なリスクのうち、情報資産に係るリスクの管理を狙いとして、情報セキュリティに関わる意識、取組及びそれらに基づく業務活動を組織内に徹底させるための仕組み（経営者が方針を決定し、組織内の状況をモニタリングする仕組み及び利害関係者に対する開示と利害関係者による評価の仕組み）を構築・運用すべきである。産業構造審議会情報セキュリティ基本問題委員会では、この取組を「情報セキュリティガバナンス」と定義している[3]。

1.2. 適用範囲

ガバナンスの適用範囲としては、個別企業、連結ベースの企業グループ、さらにバリューチェーンを形成する企業グループのいずれの捉え方も可能である[4]。特に我が国では連結ベースの統制が求められていることから、これをガバナンスの単位として扱うことが少なくないと考えられる。

1.3. 位置付け

1.3.1. コーポレートガバナンス、IT ガバナンスと情報セキュリティガバナンス

コーポレートガバナンスの定義は一律ではないが[5]、例えば「『株主による経営層の統治』と『経営層による企業内統治』の二重の統治構造により成り立つものであって、『株主による経営層の統治』が有効に機能するためには、『経営層による企業内統治』が有効に行われ

---

[3]産業構造審議会情報セキュリティ基本問題委員会「中間とりまとめ～企業における戦略的な情報セキュリティガバナンスの確立に向けて～」, 2008/06 http://www.meti.go.jp/press/20080620005/20080620005.html

[4] さらに、ネットワークでつながりうる潜在的な顧客についても企業や企業グループと相互に影響する関係にあり、情報セキュリティガバナンスを検討するうえで不可欠な経営環境の一つとして捉えることが望まれる。

[5] 「経済効率性を改善し、成長を促進し、投資家の信頼を高める上での重要な要素」「会社経営陣、取締役会、株主及び、ステークホルダー（利害関係者）間の一連の関係に関わるもの」「会社の目標を設定し、その目標を達成するための手段や会社の業績を監視するための手段を決定する仕組みを提供するもの」（OECD「コーポレート･ガバナンス原則」,2004）「企業経営を規律するための仕組み」（経済産業省「企業行動の開示・評価に関する研究会中間報告書「コーポレートガバナンス及びリスク管理･内部統制に関する開示･評価の枠組について　ー構築及び開示のための指針ー」, 2005/08/31)、「企業は、CSR を重視し、株主と同時に多様なステークホルダーに配慮した経営を行なっていく必要があり、企業が社会の公器としての役割を担っているとの視点を重視」（日本経済団体連合会「我が国におけるコーポレート・ガバナンス制度のあり方について(概要)」,2006/06/20）など。

ることが前提となる」[6]という解釈が可能である。

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確立され、その構造を踏襲するものと考えられる。ただし、情報セキュリティガバナンスの対象は、IT のみならず、組織が価値を認めるあらゆる情報資産が該当する。これは、すなわち企業の情報セキュリティ確保が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ことと整合している。したがって、情報セキュリティガバナンスと IT ガバナンス[7]は、一方が他方を包含する関係ではなく、一部重複するが明確に異なる関係となる。コーポレートガバナンス、IT ガバナンス、情報セキュリティガバナンスの関係を図 1-1 に示す。

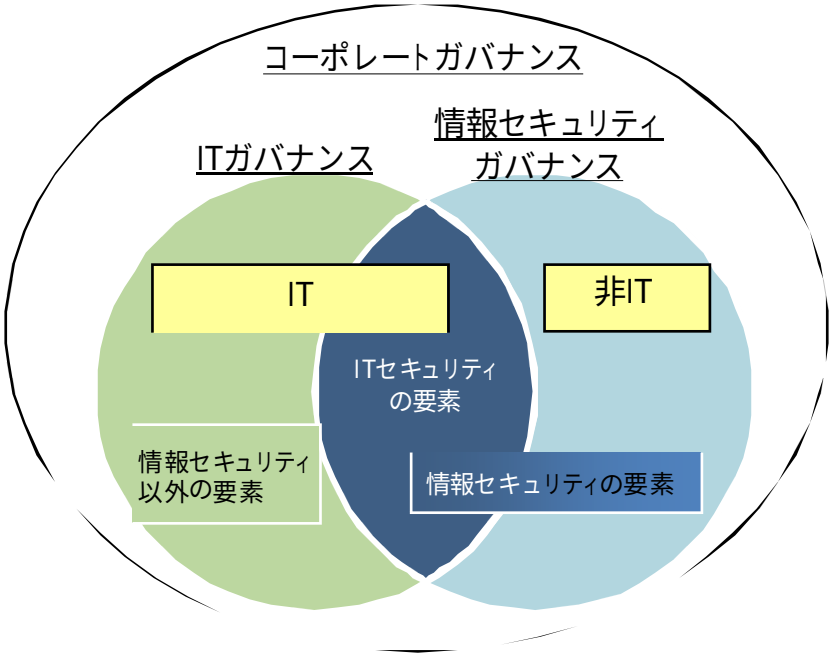


図 1-1 コーポレートガバナンス、IT ガバナンスと情報セキュリティガバナンスの関係

1.3.2. 情報セキュリティマネジメントシステムと情報セキュリティガバナンス

企業の情報セキュリティ管理手法としては、ISO/IEC 27001:2005 において ISMS（情報セキュリティマネジメントシステム）として体系化されており、その中で、「Management commitment（経営陣のコミットメント）」が求められている。

情報セキュリティガバナンスは、「経営者が方針を決定し、組織内の状況をモニタリングする仕組み及び利害関係者に対する開示と利害関係者による評価の仕組みを構築・運用すること」であり、経営陣が ISMS における「コミットメント」を行う上での活動に該当す

[6]間藤大和、平野俊明、中村直人「監査役ハンドブック」,2007/10

[7] Information Systems Audit and Control Association / IT Governance Institute「COBIT 4.1」によると、IT ガバナンスとは、「経営陣および取締役会が担うべき責務であり、IT が組織の戦略と組織の目標を支え、あるいは強化することを保証する、リーダーシップの確立や、組織構造とプロセスの構築」とされる。

る。

したがって、情報セキュリティガバナンスのフレームワークは、企業において情報セキュリティマネジメント活動を進める上での、経営陣の観点から見た行動指針やそのために必要な仕組みについて明確化したものと位置付けられる。

1.4. フレームワーク

1.4.1. 前提

1.3.1 で述べたとおり、情報セキュリティガバナンスと IT ガバナンスの位置付けは異なるが、実務上は多くの職員が両方の業務に携わることを考慮すれば、そのフレームワークは整合がとれていることが望ましい。したがって、本書では、IT ガバナンスの国際標準である ISO/IEC 38500:2008（Corporate Governance of Information Technology）が示す IT ガバナンスのモデル（付録 1）を参照する。

また、情報セキュリティガバナンスは、情報セキュリティ活動のフレームワークである情報セキュリティマネジメントシステムと整合し、全体最適化に寄与する構造であることが求められる。

1.4.2. フレームワークの構成

情報セキュリティガバナンスのフレームワークは、経営戦略やリスク管理の観点から行う「方向付け（Direct）」、ガバナンス活動の状況を指標に基づき可視化する「モニタリング（Monitor）」や結果を判断する「評価（Evaluate）」、これらのプロセスが機能していることを確認する「監督（Oversee）」、結果を利害関係者等に提示する「報告（Report）」の 5 つの活動から構成されるものとする（図 1-2）。このうち、「Direct」、「Monitor」、「Evaluate」は、ISO/IEC 38500:2008 で提示されている IT ガバナンスモデルの中の、Director が統括すべきタスクを参照している。

図 1-2 に示される、情報セキュリティガバナンスのフレームワークには、「方向付け」「モニタリング」「評価」の基本サイクルがあり、これに基本サイクルの取組を確認する「監査」や評価結果等を利害関係者に説明する「報告」といった活動を加えた構成になる。なお、利害関係者は企業の取組を踏まえ、取引先や投資先としての選別・選定を行うが、この活動は、企業として統制・管理できる範囲ではないので、フレームワークには含めない。

情報セキュリティガバナンスの「方向付け（Direct）」は、ISO/IEC 27001:2005 における「経営陣のコミットメント」の実施であり、定められた方向性の実現を目的としてマネジメントシステムの PDCA が稼動する。また、情報セキュリティガバナンスの「モニタリング（Monitor）」の対象は情報セキュリティマネジメントシステムの PDCA の状況であり、「評価（Evaluate）」では「モニタリング（Monitor）」で集約した情報から「方向付け（Direct）」

の達成度を評価し、その改善を図る。

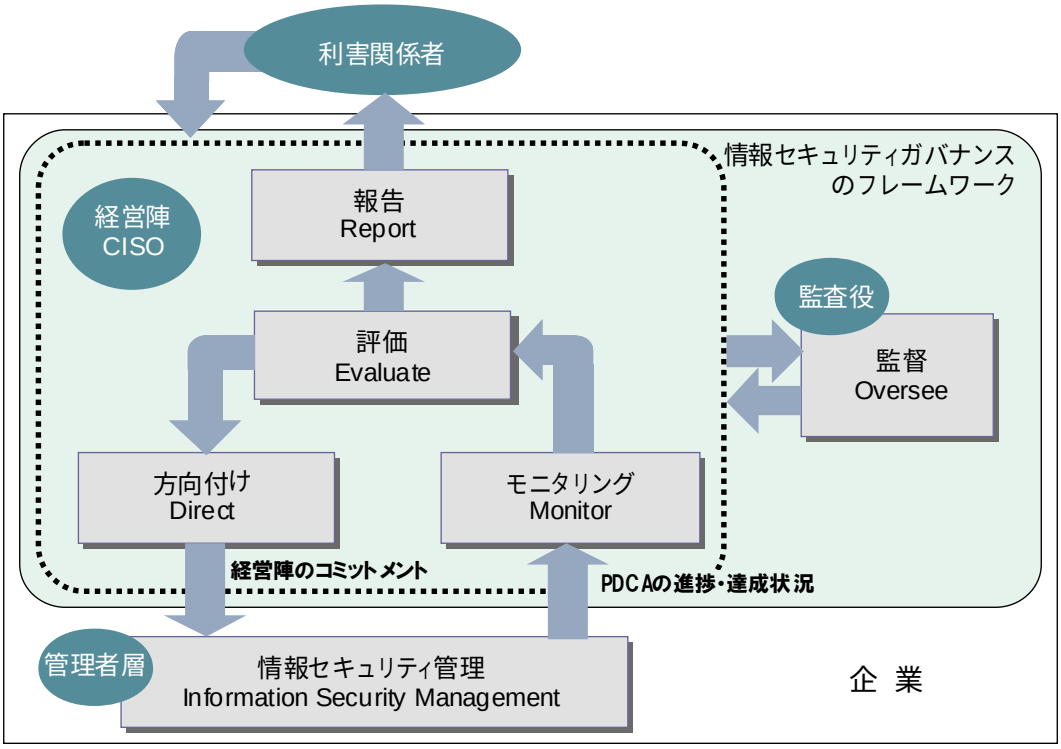


図 1-2 情報セキュリティガバナンスのフレームワーク

また、情報セキュリティ分野では監査役や利害関係者がリスク管理の観点から把握すべき事項を多数含んでいることを踏まえ、「監督（Oversee）」、「報告(Report)」という活動をフレームに組み込んだ。情報セキュリティガバナンスの確立とは、こうした活動を企業内に実装していくことに等しい。

(1) 方向付け（Direct）

経営陣は、企業価値の向上と社会的責任の遂行のために、適法性・適正性に配慮した上で、経営戦略やそれに基づくリスク管理の方針を提示する。リスク管理の方針とは「様々な経営リスクを横断的に捉え、どのリスクにどのような姿勢で取り組むのか（どの程度のリスクまで許容するか）を示す」ものである。これは、会社法で大会社と委員会設置会社に義務付けられているリスク管理体制の整備の基本方針そのものではないが、その一部として、企業がリスクと対峙する際の目安として経営陣が提示することも可能である。

また、企業/企業グループのCISO（Chief Information Security Officer）[8]が、経営若し

[8] 「情報セキュリティ対策を実施する上での責任者となる最高情報セキュリティ責任者」（「人材育成・資格制度体系化専門委員会報告書」情報セキュリティ政策会議,2007/01）。役員級若しくは部長級の人材が担当するケースが多い。企業によっては、CIO(Chief Information Officer)やCSO(Chief Security Officer)、CPO（Chief Privacy Officer）が兼ねるケースもある。

くはそれに近い立場からこのリスク管理方針を情報セキュリティ分野において解釈し、情報セキュリティ目的・目標と、その実現に必要な体制（権限や責任）や経営資源の提供を設定する。

情報セキュリティ目的とは「リスク管理方針の実現に向けて、情報セキュリティ分野で達成すべき最終の状態（ゴール）」であり、情報セキュリティ目標は「情報セキュリティ目的を実現するために一定の時間内に達成すべき状態（マイルストーン）のことであり、達成度を計測する指標値として明確化される」と位置付けられる。

(2) モニタリング（Monitor）

モニタリング（Monitor）は、経営陣が示した方向付けに従って、適切にリスク管理がなされていることを経営陣が理解できる形で示し、経営陣が評価を行えるようにするために必要な情報を収集する活動であり、CISO によりモニタリングを行うために有効かつ適切な評価指標が設定されることが必要である。

経営陣は、方向付け（Direct）の前提となる経営環境（市場、法制度、経営資源、競合環境、技術等）の変化をモニタリングするとともに、CISO から投資効果の指標や情報セキュリティ目的・目標の達成度評価の報告を受ける。CISO は、情報セキュリティマネジメントの一連の活動（PDCA[9]）の進捗・達成状況等と併せて、投資効果や情報セキュリティ目的・目標の達成度を把握するのに有効な指標によってモニタリングを行う。

(3) 評価（Evaluate）

評価（Evaluate）は、方向付け（Direct）した方針や情報セキュリティ目的・目標が実現できたかどうかを評価する活動である。

経営陣は、リスク管理方針が達成できたか、リスクが変化していないかを評価する。リスク管理方針に現実性が乏しく達成困難である、あるいは新たなリスクが顕在化している場合には、必要に応じてリスク管理方針を見直し、方向付け（Direct）をやり直すことになる。CISO は、情報セキュリティマネジメントの PDCA が的確に実施されたか、体制や経営資源は適切であったか、情報セキュリティインシデント[10]は減少したか、法令違反は起きていないか、結果として情報セキュリティ目的・目標が達成できたかを評価する。情報セキュリティ目的・目標が未達の場合には、その原因を分析するとともに、必要に応じて情報セキュリティ目的・目標を見直すことになる。

[9] Plan-Do-Check-Act（計画、実行、確認・評価、改善）といった一連のマネジメントサイクルのこと
[10]望まない単独若しくは一連の情報セキュリティ事象、又は予期しない単独若しくは一連の情報セキュリティ事象であって、事業運営を危うくする確率及び情報セキュリティを脅かす確率が高いもの（JIS Q 27001:2006）

(4) 監督（Oversee）

監督（Oversee）は、方向付け（Direct）、モニタリング（Monitor）、評価（Evaluate）が適切に遂行していることを確認し、必要に応じて問題の改善を促す監査等の活動である。

なお、その実装に際しては、業務執行者を監督する制度が国によって異なることに配慮する必要がある。我が国では、監査役制度を踏まえ、監査役監査を軸とした実装が考えられる。

(5) 報告（Report）

経営陣は、株主、取引先や顧客、従業員、社会全体を含めた利害関係者に対し、リスク管理の責任者として、情報セキュリティに係るリスク管理の状況について報告する。これらの情報は、利害関係者が当該企業の価値について評価し、取引先や投資先の選別・選定を行うためのものである。

1.5. 本書の利用について

1.5.1. 本書の狙い

情報セキュリティガバナンスの概念を企業において実現する際に問題が生じるのは、経営陣と管理者層・従業員層の間でリスクや対策についての共通認識が乏しく、役割と責任があいまいなままで、全体最適化された構築・運用がなされていないといった場合である。

一般に、経営戦略やリスク管理の方針に沿った情報セキュリティ上の目標設定、経営陣が状況を把握するためのモニタリングの仕組みの整備について具体化する有力な方法論が乏しいため、情報セキュリティガバナンス確立への有効なフレームワークの整備が求められているといえる。

そこで、本書ではこれらの課題への対処指針を明示するとともに、経営戦略と整合的な情報セキュリティの方針と、高度化が求められる管理者層・従業員層における管理策の有機的な結合を促すことを目指す。言い換えると、本書は、情報セキュリティガバナンスの定義にある「経営者が組織内の状況をモニタリングし方針を決定する仕組み及び市場に対する開示」について、経営陣が取り組むべき行動の指針を示すものである。

情報セキュリティガバナンスに係る本ガイダンスの概念イメージを図 1-3 に示す。

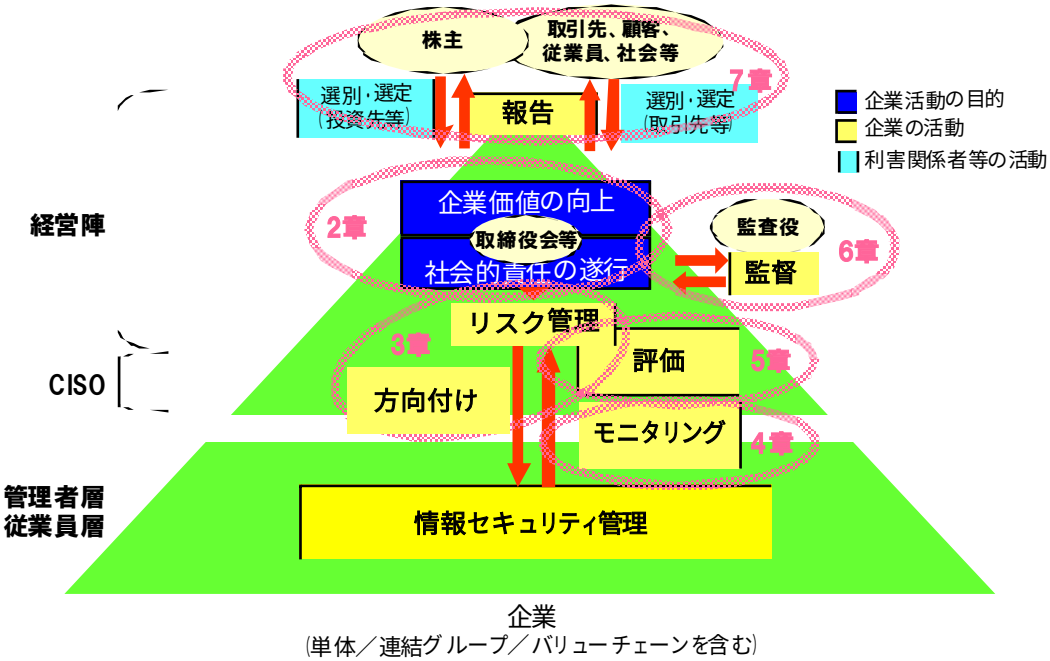


図 1-3 情報セキュリティガバナンスの概念イメージ

1.6. 本書の利用者

上記の位置付けを踏まえ、本書の想定利用者層を以下のように設定する。

- リスク管理に取り組む経営陣の方（自社への適用に取り組む際の参考書として）
- 情報や IT システムに係るリスクを憂慮し、組織内・グループ内に情報セキュリティガバナンスの確立を進める必要性を感じている経営企画、リスク管理、総務、IT 管理等の部門の方（経営陣への説明・啓発のツールとして）[11]

[11] 経営陣が「情報セキュリティガバナンスの確立を進める必要性」を認識していない、あるいは不十分であると感じている「企業の情報セキュリティ改善に責任を持っている部署・部門の担当者」の意味

2. 情報セキュリティガバナンスの効果

企業は情報セキュリティガバナンスの確立に取り組むことで図 2-1 に示すような様々な効果を得ることができると考えられる。

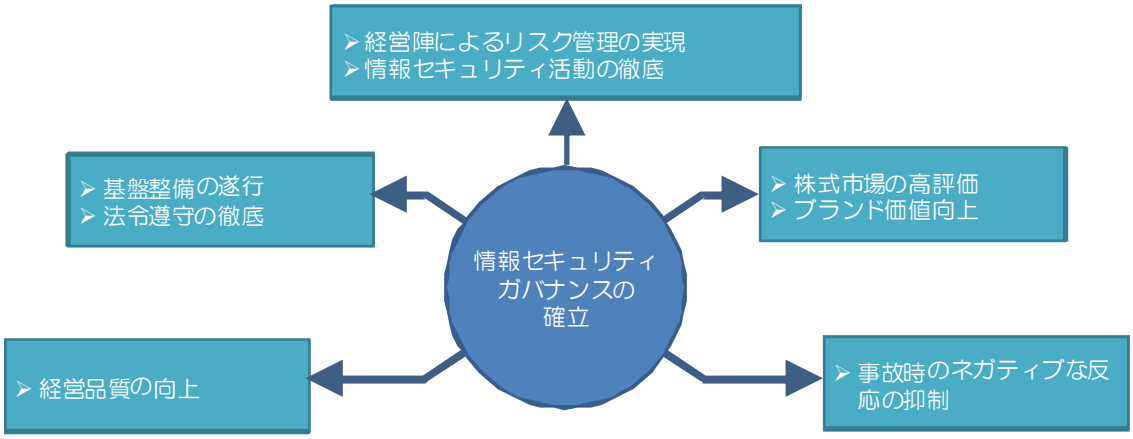


図 2-1 企業が情報セキュリティガバナンスに取り組むことで得られる効果

以降では、それぞれの効果について詳細を示す。

2.1. 経営陣によるリスク管理の実現と情報セキュリティ活動の徹底

企業が情報セキュリティガバナンスの確立に取り組むことによって得られる第一の効果は、経営陣が主導する形で情報資産に係るリスク管理を実施することで、情報セキュリティに関わる意識、取組及びそれらに基づく業務活動を組織内に徹底させることが可能となることにある。

情報セキュリティの領域では、経営陣と管理者層・従業員層との間で、リスクや対策についての共通認識が乏しく、事実上、経営陣がリスクを管理できないことも少なくない現状を鑑みれば、この効果は極めて重要である。経営陣がリスクの現状を把握できず適切な対応をとることができない状況は極めて危険な状態といえ、セキュリティ事故が企業経営に与える影響を考慮すれば、経営陣が自らリスクを判断せず、部下に判断を委ねた状況を放置している状態を健全とは言いがたい。

情報セキュリティガバナンスの確立は、こうした状況を解消し、情報セキュリティについて、経営陣がリスク管理を主導する、本来の形を実現することができる。

2.2. 基盤整備の遂行と法令遵守の徹底

次の効果として、企業がリスク管理の観点から情報セキュリティに取り組むことで、経営戦略を支える基盤整備の推進と法令遵守の徹底が期待できることが挙げられる。

例えば、情報セキュリティ対策を、従来の問題解決策としてではなく、製品・サービス提供の安定化や品質向上に有効な経営基盤の一つとして位置付けることで、その整備が企業価値の向上をもたらすことが期待できる。

また、経営陣が主導する形で、リスク管理の一環として情報セキュリティに関わる意識や取組、それに基づく業務活動を組織内に徹底させるための仕組みを構築・運用することによって、結果的に個人情報保護や内部統制強化といった企業に対する法的要請や、透明性・事業継続性の確保など、社会からの適正性に係る期待にも応えることができる。

2.3. 経営品質の向上

情報セキュリティガバナンスの確立に取り組むことで、経営品質の向上に寄与する効果も期待できる。例えば、経営品質向上プログラム[12]のアセスメント基準では、「８つのカテゴリー（経営要素）」の一つに「情報マネジメント」が挙げられており、業務能力の把握や意思決定を支援する必要な情報が適切に選択・収集され、分析されているか、さらに情報マネジメントの仕組みがどのように機能しその有効性をどのような視点から確認できるかが問われている。情報セキュリティガバナンスは、この「情報マネジメント」に対して有効なフレームワークと考えられる。

また、「経営幹部のリーダーシップ」や「経営における社会的責任」、「戦略の策定と展開」といった経営要素についても、情報セキュリティガバナンスの実効的な確立には不可欠な要素であり、情報セキュリティガバナンスの確立に取り組むことでそれらを充実させることが可能と考えられる。

2.4. 株式市場の高評価とブランド価値向上

情報セキュリティへの取組が取引先の評価に結びつき、結果として顧客の取引選好や満足度などコーポレートブランド価値に対する評価を高める効果が期待できる。

情報セキュリティに関わる商品を取り扱う業界におけるブランド調査[13]によれば、情報セキュリティ報告書を開示している企業に対して、情報セキュリティへの取組をポジティブに評価しているユーザ企業の割合は 2006 年を境に大きく上昇した。また、ユーザ企業は、取引相手を選択する際に情報セキュリティへの取組を評価項目として重んじる傾向が見られた。同様に、顧客満足度を見ても、情報セキュリティに対する取組姿勢が高い企業との取引満足度が高いという結果が得られた。

---

[12]経営品質協議会が提唱するプログラム。卓越した経営（エクセレンス）をめざして、経営全体をどの業種、業態の組織にも共通する枠組み（フレームワーク）を用いて自らの経営の状態を尺度（ガイドライン）にもって振り返ることを「セルフアセスメント」と捉え、これを活用して、経営を革新できる状態に組織の能力を高めていく。
http://www.jqac.com/NewWebSite.nsf/StaticDetailLink/1_5?opendocument

[13]伊藤邦雄・加賀谷哲之・金鉉玉「企業価値向上のための情報セキュリティガバナンス」日本企業研究センターワーキングペーパー，2009 年 1 月

2.5. 事故時のネガティブな反応の抑制

情報セキュリティへの取組を開示することにより、投資家の情報セキュリティ事故に対するネガティブな反応を抑制する効果や、顧客の安心感や取引選考への効果が期待できる。

一般に、個人情報の大量流出やシステム障害によるサービス停止など、情報セキュリティに関する事件・事故が発生した場合、当該企業の企業価値はダメージを受けることが予想される。例えば、海外の研究では、機密情報の漏えい事故の場合には統計的に有意に株価が下落することが確認されている[14]。また、他の海外の研究でも、情報セキュリティに関わる事故の報道により、企業の市場価値は有意に下落し、収益率の平均値は−2.6%となることが確認されており[15]、日本企業をサンプルにした検証でも同様の結果が得られている[16]。

また、情報セキュリティに関する事件・事故は、当該企業のコーポレートブランド価値にも影響を及ぼし得る。例えば、2001 年から 2006 年にかけて日経 4 紙で扱った情報漏えいやシステム障害など情報セキュリティに関する事件・事故が、コーポレートブランド価値に与える影響を検証した結果、事件・事故を契機にさまざまなイメージ評価が大きく低下し、5〜25%ほどコーポレートブランド価値を毀損していることが確認された。

こうした事件・事故の発生について隠蔽する、あるいは適切な説明をしないでいると、社会的評価は「事件・事故に対する不安感」から「当該企業そのものに対する不信感」へとより深刻化する可能性がある。さらに、それが開示を義務付けられている「重要事実」（金融商品取引法第 166 条 2 項で規定）にあたると見なされれば、法令違反にもなりかねない。

一方、企業が情報を開示することにより、株式市場のネガティブな反応を抑制する効果が期待できる。例えば、有価証券報告書内における「事業リスク等」の開示において、情報管理や IT に関するリスクを開示している企業と開示していない企業を比較したところ、どちらの企業も情報セキュリティに関する事件・事故を契機に株価は低下するが、当該リスクを事前開示している企業の株価はその後数日間で元の水準に戻り、非開示企業の株価は長く低迷することが確認されている[17]。

事前開示企業の株価が回復する理由として、事件・事故発生後、投資家が投資意思決定判断を見直すにあたり、当該企業の有価証券報告書を再度検討している可能性がある。つ

---

[14] Campbell. K, L.A. Gordon, M. P. Loeb, and L. Zhou, (2003) “The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market,”Journal of Computer Security, Vol.11:431-448.

[15] Cavusoglu, H., B. Mishra, and S. R Aghunathan, (2004)“The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers, ”International Journal of Electronic Commerce,Vol.9 No.1:69-104.

[16] Ishiguro, M., H. Tanaka, K. Matsuura, and I. Murase,(2006）“The Effect of Internet Security Incidents on Corporate Value in the Japanese Stock Market,” Proceedings of The 2006 Workshop on the Economics of Securing the Information Infrastructure.

[17]金鉉玉「リスク情報の事前開示が投資家の意思決定に与える影響ー情報流出リスクの顕在化ケースを用いてー」『一橋商学論叢』Vol.2 No.2, 2007 年 11 月

まり、投資家は情報セキュリティに関する事件・事故に対してネガティブに反応する傾向があるものの、あらかじめ情報セキュリティに関する開示を行っておくことで、そうしたネガティブな反応を抑制することが可能となる例である（開示に関する考慮事項としてP.2の脚注1を参照すること）。

3. 方向付け

経営陣は、企業価値の向上、適法性、適正性、社会的責任等を考慮した上で、経営戦略やそれに基づくリスク管理の方針を打ち出す。各領域の責任者がそれを踏まえた目的・目標を設定し、CISO はそれに沿って、情報セキュリティの目的・目標を設定、さらに管理者層はそうした目的・目標を実現する情報セキュリティ管理目的・管理策を策定・実施する。

3.1. リスク管理方針の決定

本節において主体的な立場を果たすのは経営陣であり、考慮すべき事項は企業全体としてのリスク管理の方針である。情報セキュリティに特化した管理策については、CISO が主体的な立場を果たす次節以降において記述するものとする。

3.1.1. 企業に求められるリスク管理

会社法では取締役に善管注意義務が課せられているが、特に大会社及び委員会設置会社の取締役に対して内部統制システム構築の基本方針の決定を明文の義務としている（付録 2 参照）。取締役には企業の価値を向上させる責務があり、リスク管理には「取締役の職務の執行が法令及び定款に適合することを確保するための体制（法 362 条 4 項 6 号）」と示されていることに象徴されるような、コーポレートガバナンス及び内部統制の体制構築が含まれると考えられる。

会社法施行規則では「損失の危険の管理に関する規程その他の体制（施行規則 100 条 1 項 2 号）」として、広義のリスク管理体制が要請されているが、整備すべきリスク管理体制の具体的な規定は明示されていないことから、リスク管理への対応には関連する複数の分野の解釈が適用されている。

例えば、社団法人日本監査役協会の「内部統制システムに係る監査の実施基準」[18]では、監査役の責務として、リスク管理体制の整備と運用についての監査やリスク分析・評価等についての監査を挙げており、経営者には、リスク管理体制の整備と実施が要請されていると解釈している（参考２参照）。

3.1.2. 企業を取り巻くリスク

一般的に、リスクは、利益と損失のいずれかが発生する「投機的リスク」と、損失のみをもたらす「純粋リスク」に分けられる。これを企業活動の観点から見ると、前者は、企業価値向上のため、成功と失敗の可能性を天秤にかけて経営者が意思決定する経営判断のリスクであり、ビジネス戦略（新規事業、企業買収・提携等）やマーケティング戦略（市場ニーズ対応、価格戦略）等に関するリスクが該当する。一方、後者は、企業内部に管理

[18] http://www.kansa.or.jp/PDF/el001_070405b.pdf

体制を構築し、損失の発生を抑制すべきリスクであり、法令遵守、情報管理、経理・財務管理、労務管理、品質管理等に関するリスクが該当する[19]。

情報管理や IT に係るセキュリティリスクは、その対処が利益に直結しない「純粋リスク」に分類される。ただし、IT は企業活動を支える重要なインフラであること、また、情報管理に係る信頼性がビジネス戦略の成否や企業ブランドのイメージにも影響し得ることを考慮すべきである。

3.1.3. 企業におけるリスク管理

企業の経営者はコーポレートガバナンス／IT ガバナンスを実現する際、経営戦略に基づいて企業価値を高め、企業が直面しているリスクを適切に管理するように経営資源を投入するものと考えられる。一般に、経営者は価値の創出によって収益の最大化を図るが、この価値の創出には同時に新たなリスクが伴うことが多い。価値の創出とリスク対策に利用できる経営資源は共通かつ一定の大きさであることから、経営者は、異なる二つの目標を同じ経営資源をバランスさせて同時に実現する経営戦略を策定することが要請されているといえる。

例えば、製造業を考えると、製造ラインに IT を導入し作業の多くを自動化することで生産能力を大幅に高めることができる。しかし、導入した IT 機器に故障が発生した場合、その製造ラインの利用が全面的に停止して生産活動が継続できなくなるというリスクが発生することが予測される。そこで、経営者は IT 機器の障害により生産ラインが全面的に停止しないように、IT 機器毎の障害発生率を鑑みて、比較的障害の発生しやすい部分を冗長化する、IT 機器ベンダ指定の点検時期よりも短い期間を定期点検時期と指定する、等といったリスク対策を行わなければならない。このようなリスク対策には特別の費用や IT 関連スタッフが必要となることから、経営者は、投入する資金や従業員をどのように配分したら、どの程度の収益を上げることができるのかを考慮して経営戦略を決めなければならない。

3.1.4. 経営陣によるリスク管理方針の決定

経営陣は、経営戦略に基づくリスク管理の方針[20]を定める。リスク管理方針の決定とは、経営戦略に基づきリスクの許容レベルを設定すること、すなわち、守るべき企業価値や適法性、適正性、リソースの制約や社会的責任を考慮し、優先して対応しなければならないリスクを明確にすることである。

リスク管理方針の決定は、例えば以下の手順で実施する。

---

[19] ただし、経理・財務管理においても、資金の投資・運用という業務があるため、その面においては、利益と損失が考慮されるものとなる。また、単に「労務管理」ではなく、「人事管理」と捉えると、有能な人材の採用や登用、社員のモチベーションの向上などにより、事業における利益を生み出すこと、また採用等における判断の誤りによる損失もある。

[20] 会社法において大会社及び委員会設置会社に求められているリスク管理体制の整備の基本方針ではなく、企業としてのリスク管理そのものの方針を意味する。

1) まず、自らの価値と、経営環境に基づく脅威、さらに自社の弱み（ぜい弱性）を把握した上で、どうしても守らなければならない、企業活動の根幹に関わる価値を明確にする。企業活動の根幹に関わる価値とは、企業の業種や規模、風土等によって異なるが、例えば、生産能力、研究開発力、製品・サービスの品質、ブランド・信用等である。

2) 次に、企業活動の根幹に関わる価値が損なわれた場合の被害の大きさ（影響度）やその発生確率を想定し、対応を優先すべきリスクを明らかにする。

3) さらに、そうしたリスク対応に関する基本的な姿勢を定める。リスク対応の方向や体制・予算等の配分は、企業の経営環境やリスク状況に応じて経営陣が判断すべきものである。リスク対応には、例えば合理的な範囲で事故発生可能性の低減に努める、ビジネスモデルを変更してでも事故発生を回避する、事故発生に伴う損失の局限化を図るといった方向を選択する。また、決定されたリスク対応に必要な経営資源を確保することは経営陣に求められる重要な任務である。

経営陣が定めたリスク管理方針は、リスクの関連分野の最高責任者によって、その分野に即した形で解釈され、具体的な目的・目標に展開される。企業が抱えるリスク分野は、情報セキュリティ以外にも、法令遵守や製品・サービス安全、環境保護、防災など多岐にわたることから、各分野の最高責任者がリスク管理方針からそれぞれ具体的な目的・目標を設定する。さらに、目的・目標の実現を目指す形で各分野のマネジメントシステムが稼動する。

リスク管理方針と各分野の目的・目標の関係を図 3-1 に示す。

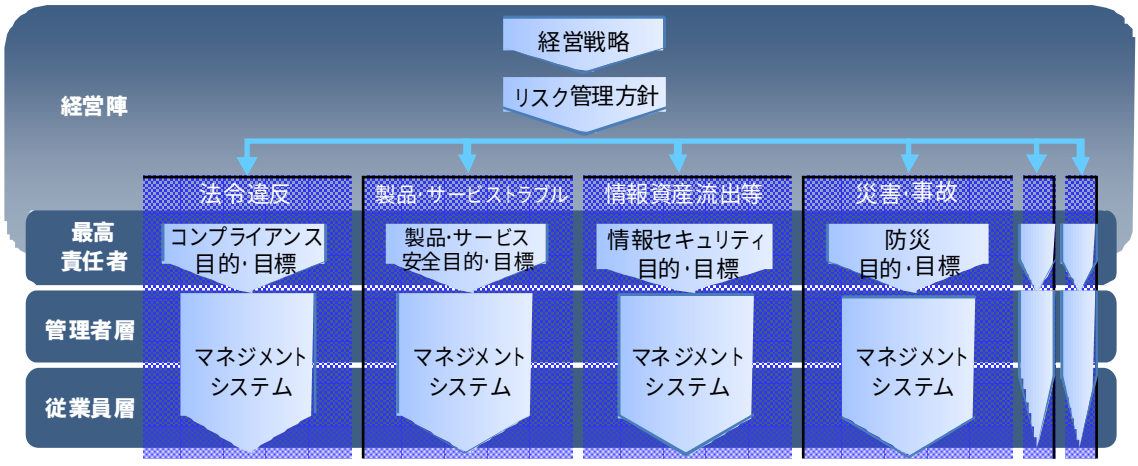


図 3-1 リスク管理方針と目的・目標の関係

3.2. リスク管理の方法論

3.2.1. リスク管理体制

従来、リスク管理は部門ごとに個別に対応していたが、リスクの多様化や影響範囲の拡大に伴い、全社的な立場からリスク管理を行う必要が増している。しかし、企業において問題が発生した際、現場から経営陣への報告が遅れる、あるいは経営陣の状況把握や意思決定に時間がかかることで対応が遅れ事態を悪化させてしまうことがある。そこで、そうした情報を集約し、経営陣に報告するリスク管理部門を設置するケースが見られる。すなわち、現場で事件や事故が起きると、これらの情報はリスク管理部門に集約され、初期対応を含めた形で経営陣に速やかに知らされる。経営陣は、リスク管理部門からの情報に基づき、一次対応、二次対応と矢継ぎ早に対応を行うことで、問題が拡大することを防いでいる。

図 3-2 は、このような全社的なリスク管理体制の例である。情報セキュリティについても、リスク管理の仕組みの一環として機能するものであることが望ましい。

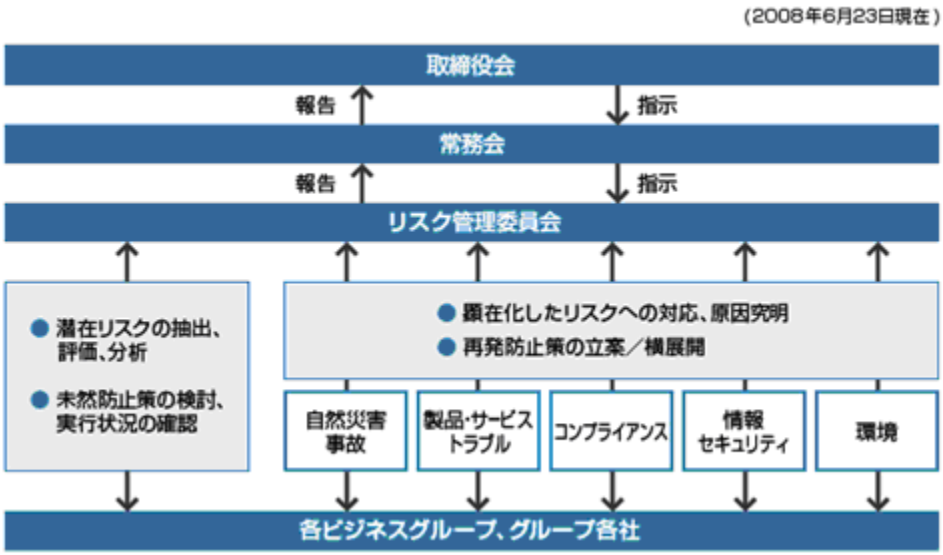


図 3-2 リスク管理体制とリスクマネジメントサイクル[21]

しかし実際には、「経営陣から見て状況や課題が理解できず評価が難しい」、「管理者層・従業員層から見て経営陣の提示する方針に具体性が乏しくどのように実装すべきかわかりにくい」など、経営陣と管理者層・従業員層の間に存在するギャップから生じる各種の問題が指摘されている。

このような問題を解消する方法として、経営陣と管理者層・従業員層の間をつなぐ仲介

[21]出典：「2008 富士通グループ 社会・環境報告書」

者を設置することが有効と考えられる。その仲介者の役割を担うのが、経営若しくはそれに近い立場から企業/企業グループの情報セキュリティを統括する責任者、すなわち CISO である。CISO がリスク管理方針から情報セキュリティ目的・目標を展開し、経営陣の意思を反映した対応策の実装を可能にする。CISO は経営陣の一員、若しくは経営トップからその役を任命された管理者であり、組織内からその任務を認識されていることが重要である。

さらに、各部門に情報セキュリティ管理責任者を任命する、組織内の情報セキュリティに関する調整と意思統一を行う『情報セキュリティ委員会』を設置する、といった、情報セキュリティマネジメントに必要とされる体制を整備することが望まれる。その際、経営陣及びCISOには、情報セキュリティを管理する単位と対象範囲について明確にすること、経営管理や品質管理など他の組織活動との位置付けの明確化と連携方法を検討すること、委員会には担当役員、情報セキュリティ管理責任者など情報セキュリティの関係者だけでなく、情報システムや法務、総務、人事など関連の深い部署からもメンバーを参画させることなどが求められる。

3.2.2. リスクマネジメントモデル

リスクマネジメントは、リスクを低減等し、継続的に受容できるレベル以下に保つことを目的とした活動と考えることができる。環境問題や製品安全、情報漏えいなど、企業が抱えるリスクは多様化している。その結果、リスク管理を個々の事業における問題として扱うのでは十分といえないため、ISO 31000[22]や COSO-ERM[23]といったリスクマネジメントのモデルが提唱されている（付録 4 参照）。

また、セキュリティマネジメントのフレームワークとしては、国際標準である ISO/IEC 27001:2005、米国の連邦情報セキュリティマネジメント法 (FISMA：the Federal Information Security Management Act)に基づくリスクマネジメントフレームワークとそれを構成する FIPS 文書[24]・NIST SP800 シリーズ[25]などが活用可能である。

3.3. 情報セキュリティ目的・目標の設定と管理策への展開

本節において主体的な立場を果たすのは CISO であり、考慮すべき事項は企業全体としてのリスク管理方針に基づいた情報セキュリティ目的・目標となる。

---

[22] 「Risk management - Principles and guidelines （リスクマネジメント－原則及び指針）」という標題で現在検討されているリスクマネジメントの国際標準案。あらゆる組織のあらゆるリスクを対象とする。2009 年 10 月に国際規格として発行される予定。

[23] COSO（米トレッドウェイ組織委員会）が打ち出した企業リスクマネジメントのフレームワーク（Enterprise Risk Management-Integrated Framework）。COSO は内部統制の枠組みを定めた委員会であり、2004 年 9 月に公表された改訂版（COSOⅡ）の中で ERM を提案した。

[24] Federal Information Processing Standards: 米国連邦標準規格。

[25] 米国国立標準技術研究所(National Institute of Standards and Technology)で発行するコンピュータセキュリティ関係のレポート。セキュリティマネジメント、リスクマネジメント、セキュリティ技術、セキュリティの対策状況を評価する指標、セキュリティ教育、インシデント対応など、セキュリティに関し、幅広く網羅している。

3.3.1. CISO による目的・目標設定

経営陣が打ち出したリスク管理方針を基に CISO は情報セキュリティ目的・目標を設定する。情報セキュリティ目的とは「リスク管理方針の実現に向けて、情報セキュリティ分野で達成すべきゴール」である。また、情報セキュリティ目標とは「情報セキュリティ目的の達成度を評価できるように定める、情報セキュリティ目的の指標」である。情報セキュリティ目標の設定に際しては、その達成度を評価し経営陣に報告する必要があること、管理者層が目標を具体的な管理策に展開することに配慮することが望まれる。

以下に、リスク管理方針から情報セキュリティ目的・目標を展開するイメージを例示する。

【例：製造業中堅 A 社】

研究開発力で同業他社に対して競争優位性を持ち、グローバルサプライチェーンに参加する A 社では、想定される深刻なリスクとしてサプライチェーン傘下の企業からの信頼を失うことが挙げられる。また、事業継続性を高めることで、対外的な信頼を高め、企業活動そのものを促進することも期待している。したがって、A 社の経営陣はリスク管理方針の「企業活動の根幹に関わる価値」として以下を打ち出して、そのための体制や予算等の経営資源を割当てる方針を示した。

- 取引先からの信頼の維持・向上
- サプライチェーン間のネットワーク障害に対応する企業間連携体制の整備

これに対し、A 社の CISO は、情報セキュリティ目的として以下を掲げた。

- 共有する技術情報の保護
- 製造ラインの事業継続性の確保

さらに、共同開発を前提として、以下を要件に追加した。

- 機密データの共用やリモートアクセスといった利便性はできる限り維持しつつ安全性を保つ
- 製造請負事業の積極展開に資する信頼性強化

次に、CISO は、情報セキュリティ目的の達成度の指標となる情報セキュリティ目標として、以下の項目を掲げた。

- 他社との共有資産である技術情報を含む重要情報が明確に区分され、会社の定め

る規程に則り適切に管理されること

- 情報管理規程が遵守されていること
- 情報システムの停止や処理能力の著しい低下が発生した場合にも、最低限の生産体制が維持できるよう、適切かつ合理的な方策が適用されていること
- 製造ラインの IT 汎用技術導入に応じて適切な情報セキュリティ管理策を適用すること

3.3.2. 管理者層による情報セキュリティ管理目的・管理策の設定

管理者層は、CISO から提示された情報セキュリティ目的・目標を受け止めて、それを実現するための情報セキュリティ管理目的・管理策を設定する。これらを設定することにより、情報セキュリティポリシーや具体的な管理策の選択・構成の枠組みを定めることができる。

3.3.1 に示した A 社の例で言えば、情報セキュリティ管理目的として以下のような項目をあげることができる。

- 情報の区分と取扱の規程が組織横断的に適用され、分類がなされていること
- 分類された情報が各現場において取扱規程に則った管理が実施されていること
- 重要情報の取扱規程に関する従業員教育が実施されていること
- 重要情報の取扱規程が現場の業務フローと整合していること
- 従業員の PC のセキュリティ設定が会社の共通ルールに適合していること
- 従業員の PC には、許可なく USB メモリを利用しないこと
- 共同開発を行う協力会社と守秘義務契約を締結するとともに、同社の担当者から NDA（機密保持誓約書）の署名を得ること
- 製造ラインの基盤 IT システムに関する事業継続計画を策定・維持すること
- 製造ラインの IT 汎用技術に関するリスク分析の実施及び対策を適用すること
- ネットワーク管理規程が定められ、そのための従業員教育がなされていること。
- インシデント対応態勢が整えられていること

管理策とは、リスクを低減するために組織内で実施される方策である。組織は自ら定めた情報セキュリティ目標を達成するためには、適切な管理策を選択し、それを正しく実施し、その有効性を評価することが必要である。特に管理策選択が適切であることは、その組織内の情報セキュリティ対策の有効性及び効率性に直接の影響を及ぼす。

組織内で選択される一連の管理策がそれぞれお互いに矛盾することなく整合し、また最適なバランスで配置されるようにするために、それぞれの管理策は共通した組織のセキュ

リティ上の活動目標から導き出されるのが望ましい。

例えば ISO/IEC 27001:2005 では、情報セキュリティ管理策は組織の ISMS 基本方針に基づいて運用される情報セキュリティマネジメントシステム（ISMS）の活動の一環として選定される。ISMS の各プロセスが正しく運用されることにより、経営者が策定した ISMS 基本方針に従った管理策が選定されることが保証される。したがって、ISO/IEC 27001:2005 に従ったマネジメントシステムにおいては、ISMS 基本方針と組織の情報セキュリティ目的・目標を正しく対応付けておく必要がある。

また、従来、技術的管理策は、その導入により情報セキュリティリスクを排除・低減すること、すなわち管理策としての「有効性」に議論が偏りがちであり、リスク分析の結果を踏まえつつ、その管理策によって得られる効果が投下したコストに見合っているかという「効率性」の議論はあまり行われてこなかった。しかし、情報セキュリティガバナンスの観点で考えるならば、これらの技術的管理策について「有効性」だけではなく、リスク分析の結果を踏まえた「効率性」も相応の重要性を持ってあわせて検討することが求められるであろう。

【トップダウンとボトムアップ】

組織に情報セキュリティ対策を実装する際には、企業グループ全体を対象として情報セキュリティ対策のデザインを描いて導入することが理想的である。そのためには、トップダウンで情報セキュリティに対する取組の方針や原則を経営者が示し、その方針や原則に基づいて各組織レベルで情報セキュリティ対策を実施していくことになる。

ただし、複数事業、地域的な分散があるような大きな組織の場合は、組織全体として定めた原則的な対策が個々の局面においては現実にそぐわない面も生じる。そのような場合は、組織全体の方針や原則にできる限りそった範囲、一定のリスク水準を担保したうえで例外的な取扱として認めていく必要がある。情報セキュリティ対策の実施は、ビジネスの成功を目的としたものであり、ビジネスを過度に萎縮させ全体としてビジネスの発展や成功を阻害するようになっては本末転倒である。そのために個々のビジネス環境に応じたセキュリティ対策をボトムアップで改善していくことが重要となる。全体としての統一感をもったセキュリティ対策のデザインを描くことは重要であるが、ボトムアップの対策レベルの改善もまた重要である。日本の企業では、現場における品質管理サークルを通じてさまざまな経営改善を行っている企業が多い。情報セキュリティ対策を現場での品質管理サークルを通じて改善していくという手法も考えられる。そのためには、セキュリティ対策に取り組む現場の担当者のモチベーションを向上させることが不可欠である。

3.4. 個別の課題

3.4.1. 企業グループのセキュリティ

金融商品取引法の適用により、上場企業を核とする企業グループには、財務報告に係る内部統制強化が求められている。そのため、財務情報については横断的に統制を利かせることができるようになった。

しかし、情報セキュリティについては、業種や企業規模、予算、人材の有無、情報資産の構成、IT への依存状況、情報管理や IT に係るリスク等、置かれている環境が様々なグループ各社において同じ対策を一律に適用することは合理的でも現実的でもないことから、各社の判断で情報セキュリティ対策を行わざるを得なく、グループ全体としての統制がとれていないケースも多いと考えられる。ただし、グループ企業のいずれかで、一度でも情報セキュリティに係る事件・事故が発生すれば、その影響は一社にとどまらず、グループで共有するブランドの信頼性が損なわれ、グループ全体がダメージを受ける可能性がある。したがって、グループ経営の観点から見れば、企業グループにおいては、財務情報にとどまらず、すべての価値ある情報について、横断的な情報セキュリティガバナンスを確立する必要があると考えられる。

統制の適用手段には、出資による経営権と契約のいずれか若しくは両方が想定される。基本的には、経営権を有し統制可能な子会社についてはグループ統制への対応を要請し、そうでない企業については契約ベースでの対応を求めることになる。

ただし、50%以下の出資先に対しての要請や、複数の出資元からの要請がある場合の被統制企業としての対応については、状況に応じた対処が必要である。例えば、複数のグループ企業から、自社の業務遂行上、重要な関係企業として位置付けられている場合には、それら各社と調整して、それぞれの要請を可能な限り共通化・汎用化し効率的な対処を図る、あるいは社内において業務プロセスやプロジェクトごとに、格付あるいはラベル付けされた情報の流通を制限するファイアウォールを設けて厳格な情報統制を行う、といった対応策が適用される。

また、連結対象の企業だとしても、その企業の情報セキュリティレベルがその他グループ企業のものと大きく乖離している場合やグループの情報セキュリティ方針に従わない（費用の制約等から従うことができない）ため、グループが求める情報セキュリティに係る統制が困難な場合などは、グループの情報セキュリティ方針の徹底という観点から経営判断として連結対象から除外するなども１つの対応策として考えられ、そういった対応を行っている企業も存在する。

企業グループにおける情報セキュリティガバナンスの確立に関するアプローチの例を以下に示す。

(1) ベースラインアプローチ

ある程度、各社の規模が揃っている企業グループの場合、横断的・共通的な情報セキュリティ目的・目標・管理策を設定して、それをクリアする条件を一律に課すベースラインアプローチの手法が有用である。

また、同じグループ内でも、規模の大きい企業は自律的に自社のリスクを把握し、必要な対策を適切に対処していて、グループとしての強力な統制が不要である場合には、規模の小さい企業について、最低限の要求事項を設定し対応を促す手法が考えられる。その際、設定するベースラインの難度によってコスト負担が増え、グループ企業の同意を得ることが難しくなる可能性もあるため、ベースラインの妥当性をどのように担保するかが重要となる。リスク管理としてどこまで求めるか、モニタリングの観点も視野に入れ、現実的・実効的な設定が望まれる。

(2) グループ企業マッピング

実際には、業種や企業規模、予算、人材の有無、情報資産の構成、IT への依存状況、情報管理や IT に係るリスクなどが大きく異なる企業グループの場合、対策を一律に適用することは現実的ではない。

その場合、グループ企業各社の抱えているリスク等に基づき、各社を分類することで、それぞれに求められる対策レベルと現状とのギャップを明示し、対策を促す手法を適用することができる。

具体的には、共通の分類軸を設定して、グループ各社を評価し、いくつかのタイプに分類する。次に、グループとしてのリスク管理方針、情報セキュリティ目的・目標に基づき、それぞれのタイプに求められる情報セキュリティ要件を規定する。その上で、タイプごとに情報セキュリティ要件と各社の現状とのギャップを計測し、各社に対応を求める[26]。ただし、グループ各社の事業活動やリソースによって対応が困難なケースもあることから、統括会社は各社と協議の上で優先順位を設定し、柔軟な姿勢で取り組むことが望ましい。

(3) IT 基盤や体制の共通化・統合化

グループ各社が、異なるシステムや体制を採用していると、横断的・網羅的なチェックに手間や時間を要し、事故や不正のリスクを見逃す可能性が高まる。また、グループ全体で見れば、運用コストの重複も無駄な費用である。

したがって、リスク管理の観点からも、コスト削減の観点からも、グループ企業間で IT 基盤を共通化・統合化することは効果的である。実際の導入については、例えば、親企業

[26]独立行政法人情報処理推進機構が運営するセルフチェックサイト「情報セキュリティ対策ベンチマーク」はこのような用途に活用可能である。http://www.ipa.go.jp/security/benchmark/index.html

や有力企業の既存の IT 基盤を軸に、各社の IT 基盤の更新期を目安にして、対象範囲を段階的に拡張していく展開が考えられる。

また、情報セキュリティの啓発コンテンツや緊急対応体制（3.4.2 参照）などをグループ内で共有することもコスト面で有効である。

(4) 全社共通の規程や基準の定着

様々な業界において国際的な再編が進み、企業の買収・合併が常態化している昨今、同じグループに属する企業といっても、共通の土壌・文化を有すると考えるのは適切ではない。特に、海外のグループ企業においては、法制度や文化、商慣習などが異なるため、同じ規程や基準を適用しようとしても、実現困難である、または従業員の認識が揃わない可能性がある。

グループ企業間に共通のセキュリティポリシーを共通認識として確立するためには、統括会社から、国内外のギャップを踏まえた追加的な資料（用語集、ビデオ等）を提供する必要がある。

また、以下のような取組が有効である。

- 共通の研修やテストを通じて質の向上を図る
- グループ横断的な連携・啓発担当者が海外のグループ各社を訪問し、管理者や従業員と直接の意見交換を進めて、コミュニケーションを強化する
- グループ横断的な連携・啓発担当者が、横断的な方針・規則を現地化するよう、現地の法制度や文化、商慣習を踏まえた各種調整を行う

3.4.2. 危機管理モデル

事故前提の観点に立てば、予防策だけでなく、事後対応についても準備しておくことが重要である。

個人情報保護法の全面施行を背景に、個人情報流出については対応マニュアルを用意した企業も少なくない。しかし、トラブルの発生可能性を考慮すれば、本来はそうした状況設定を情報セキュリティに係る事件・事故全般まで広げて検討すべきところである。

また、社外のデータセンターを活用するなどしてリスク移転をしている場合でも、委託先が関わるトラブルが発生した場合には、その監督責任が問われることから、いずれにせよ危機管理体制が必要であることにも留意すべきである。

情報セキュリティガバナンスの確立の際には、このような危機管理の課題もカバーしておく必要がある。課題の例を以下に示す。

(1) 緊急対応体制

リスク管理体制の一環として、緊急事態が発生した際には、意思決定の迅速化を図るため、経営層を軸とする危機管理委員会を発足する企業も見られる。

一方、現場スタッフのトラブル経験が浅く、被害の抑制や原因分析、影響範囲の特定などにどのような作業が必要か理解できていない場合には、トラブル処理について助言する実務的な専門家の存在が必要とされる。同時に、事業継続や復旧、再発防止といった作業についても、当事者以外の関係部署の支援・対応が必要なケースが多い。したがって、経営判断を行うリスク委員会とは別に、実務的な対応を支援する体制を整備しておくことが有効である。

具体的には、情報システム部門、総務部門、法務部門、渉外・広報部門の参画が望まれる。また、IT を中心とする情報セキュリティのトラブルについては、CSIRT（Computer Security Incident Response Team）というインシデント対応の実務チームを立ち上げることも有効である[27]。

さらに、昨今の情報システムに対する脅威や攻撃がより検出しにくい方向に進化していることから、監視や原因分析等については社外の専門家の技術を活用することも効果的である。

(2) エスカレーションと権限委譲

緊急事態において、必要なアクションが適切にとられず、被害を拡大したり、解決を長引かせたりすることがある。例えば、社内 LAN 上のサーバがコンピュータウイルスに感染して、重要情報が流出する事態が発生した場合、被害の拡大を止めるためにネットワークを遮断しサービスを中断する必要があるが、現場の管理者にそのような権限がなく、その了解を得る緊急の手続きも確立されていないと、何もできない状況に陥ることになる。つまり、非常事態に重要情報保護と IT サービス継続のどちらを優先するかをあらかじめ明確にしておくとともに、そのための手続きも確立しておかなければならない。

このように、トラブル発生時にどのような基準に基づき、どのような手順で上の階層に報告し、問題に対処するかという、いわゆるエスカレーション[28]の仕組みを明確化しておくことが重要である。これにより、現場の判断に係る責任や負担感は軽減される。

ただし、上述のような一刻を争う緊急事態においては、そうしたエスカレーションを展開することでロスが生じ、事態を悪化させる可能性がある。したがって、自社の体制や環境を踏まえ、いくつかの条件下においては権限を委譲し、全社に影響を及ぼし得る意思決

[27]参考資料として、JPCERT コーディネーションセンターが提供している「CSIRT マテリアル」などがある。
http://www.jpcert.or.jp/csirt_material/
[28]対応が困難な問題が発生している場合に、より上位の階層に報告し、対応を任せること。

定を現場レベルで行うケースを認めることも検討すべきである[29]。

(3) 対外説明

事件・事故、そこまで至らないインシデントについて、どのように対外的に説明するかは経営判断の領域である。対外説明に係る自社の社会的責任と影響を勘案し、その内容や対象範囲を検討する必要がある。

なお、発生した事故・事件が金融商品取引法上の「重要事実」に該当する場合には、遅延なく開示することが義務付けられる。しかし、自発的に公表する場合、その適切なタイミングについて判断が難しいケースもある。例えば、十分な情報収集を行わないまま公表を急ぐと事実関係が不明瞭になり、情報隠蔽を疑われてしまうことになりかねない。一方、情報収集・分析が完了するのを待ったために公表が遅れると、対外説明に関する姿勢が疑問視される可能性がある。したがって、情報セキュリティに関する事件・事故の場合には、正確な分析に時間を要することに留意してスケジュールを定め、段階的な公表や定期報告を行うなど、情報開示の方法を工夫する必要がある。

[29] IT システムにおいては、全てのデータにアクセスできる特権（privilege）を持つユーザが設置されている。大規模災害等の緊急時において、このような特権ユーザが一人も活動できない状態（交通機関の停止、洪水、火災等の要因）が生じる可能性を考慮し、通常は特権ユーザとして作業を行わない者であっても、エスカレーションレベルによっては特権ユーザとして活動できる情報（ID、パスワード等）を引き出せるような仕組み。

4. モニタリング

前章では、経営陣によるリスク管理方針の決定から CISO による情報セキュリティ目的・目標、管理者層による情報セキュリティ管理目的・管理策へとトップダウンに展開される「方向付け（Direct）」について示した。本章では、その実践がどのような状況にあるかを把握する「モニタリング（Monitor）」について解説する。

以下に示すように、前章で示された、経営陣、CISO、管理者それぞれの「方向付け」した内容が適切であるか、達成状況、適用状況の実情を適時に把握することがモニタリングの目的となる。また、モニタリング結果から迅速に行動を起こすため、事前に定量的な評価指標を設けておくことが求められる。

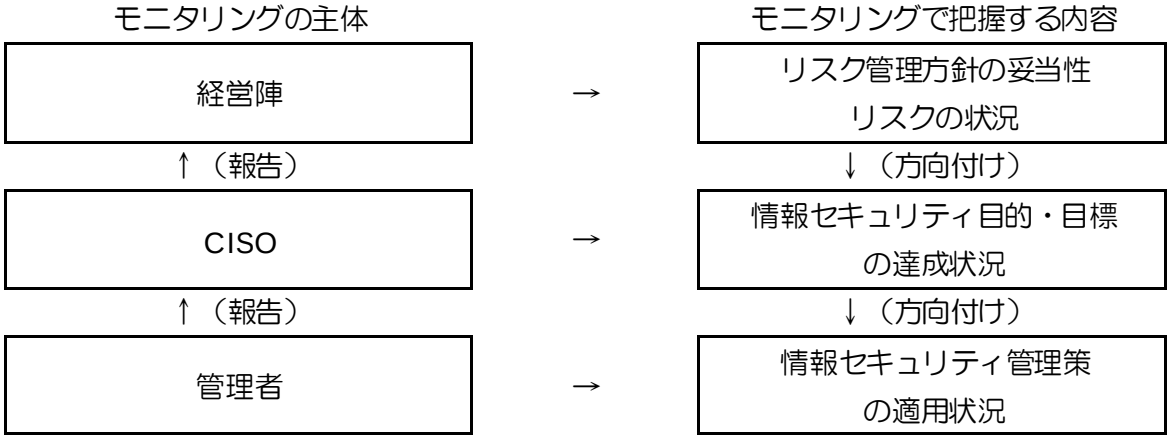


図 4-1 方向付けとモニタリングの関係

このうち、モニタリングの目的である「評価」は次章で解説することとして、本章では、モニタリングで把握する内容と、モニタリング指標の考え方について整理する。

4.1. モニタリングで把握する内容

モニタリングは、実施主体の階層によって、次のように分類できる。このうち、情報セキュリティガバナンスのフレームワークで扱うのは主に 4.1.1、4.1.2 である。

4.1.1. 経営陣が行うモニタリング

経営陣がモニタリングを行う目的は、自らが提示したリスク管理方針の妥当性を評価することにあり、そのために有効な項目がモニタリングの対象となる。例えば次の項目が挙げられる。

- 経営環境の変化
- リスクの変動や新規リスクの発生が起きているか
- 情報セキュリティ投資効果

- リスク分析の結果に照らして期待されるリスク低減の効果が発揮できているか
- 情報セキュリティ目的・目標の達成度評価
- リスク管理方針が実装できたか

経営環境の変化に関する情報は、主に経営企画部門のような事業戦略策定を行う部署が収集しており、経営会議等の会合を通じて把握することができる。

また、投資効果の指標や情報セキュリティ目的・目標の達成度評価については、CISO から経営陣に報告される。一般に、これらの報告は定期的な会合の場で、四半期～年に一回の頻度で行われることが多い。

4.1.2. CISO が行うモニタリング

CISO がモニタリングを行う目的は、情報セキュリティ目的・目標の達成度評価などを経営陣に報告することであり、そのために必要な項目がモニタリングの対象となる。例えば次の項目が挙げられる。

- 情報セキュリティ投資効果
- リスク管理方針に照らして有効かつ効率的な投資であったか
- 情報セキュリティ目標の達成状況
- 情報セキュリティ目的が達成できたか
- PDCA の進捗・達成状況
- 情報セキュリティマネジメントが機能しているか

情報セキュリティ投資効果は、経営陣への報告事項として重要なものの一つである。有効性、効率性を把握する具体的な観点としては、情報セキュリティに関する体制の活動状況、投資の有効性、事故の有無、法令遵守の状況等が挙げられる。

また、情報セキュリティマネジメントを適切に機能させることが CISO の役割であることから、CISO は管理策の実施状況や有効性評価を含む PDCA の一連の活動の進捗・達成状況を把握しておく必要がある。実際のモニタリングでは、PDCA の進捗や有効性に問題がある場合には原因と対策をレビューできるように、各組織の情報セキュリティ管理者を集めた委員会やヒアリングを通じてその状況を把握するのが一般的である。また、ISO/IEC 27001:2005（情報セキュリティマネジメントシステム）で要求されている事項（導入及び運用、監視及びレビュー、維持及び改善、文書管理等）から適切な項目を抽出して、その実施状況をモニタリングすることで、網羅性を担保できる。

4.1.3. 管理者が行うモニタリング

情報セキュリティマネジメントの一環として、各組織の情報セキュリティ管理者は、情報セキュリティ管理策の適用状況についてモニタリングする必要がある。情報セキュリテ

ィ管理策には、各情報資産に対するアクセスコントロールや、ID 管理の状況、不正ログイン回数、ウイルス対策、暗号化対策状況など IT に関するものも多く含まれることから、システム化して、そのログやイベント情報を記録・収集・加工することにより効率化と正確性の向上が可能となる。また追跡性を要求されるものについてはその記録の正当性の確保（改ざん防止、時刻同期）も必要となる。

4.2. モニタリング指標の考え方

モニタリング指標とは、モニタリングの内容を計測するデータ項目である。モニタリングの内容に応じて、それを指し示すモニタリング指標を定め、その対象範囲や収集方法等を明らかにする必要がある。

4.2.1. 測定項目とモニタリング指標の決定

組織内において、モニタリング指標を直接測定することは一般に困難である。通常は、組織内に散在する情報を収集・選択・集計・分析することにより、最終的なモニタリング指標を得る。

組織内には、モニタリング指標の情報源となる対象は多数存在する。技術的管理策からは機器の稼動状況やセキュリティに関する情報などが発信される。運用的管理策や組織的管理策からは、管理策の実行状況や実行の結果などの情報が得られる。これら管理策を直接測定して得られる情報は、一般に大量であり、またそのまま何らかの意味を直接読み取ることはできないことが多い。そのため、管理策から得られた測定情報（測定値）は評価者が理解しやすいように加工を行う必要がある。

なお、モニタリング指標は表 4-1 の特性を満たすことが望ましい。（これらの各特性の頭文字を取って「SMART」と呼ばれる。）

表 4-1 望まれるモニタリング指標（SMART）

特性	概要
Specific	測定者が測定するときに主観や判断が入らないように、あいまいな言葉を使わずに明確にモニタリング指標が定義されていること。
Measurable	本質的に数値化できるモニタリング指標であること。
Attainable	予算や技術的な制約の中で継続的に取得可能なモニタリング指標であること。
Repeatable	測定者や測定時期、測定場所などが異なっても、同じ対象を測定すれば同じモニタリング指標の値が得られること。
Time Depend	固定した値ではなく、時間と共に変化するモニタリング指標であること。

情報セキュリティ管理策に基づくモニタリング指標の例を表 4-2 に示す。

表 4-2 モニタリング指標の例

分野	モニタリング指標の例
人的・組織的セキュリティ	情報セキュリティ委員会の開催数と参加率
	情報セキュリティ教育の受講者数と受講率
情報資産	情報資産リストの登録数と適用率
	リスクアセスメントの実施数と適用率
	PC 管理規程の見直し回数
システム開発	セキュリティ要件定義書の策定数と適用率
	Web アプリケーションセキュリティガイドラインの適用数と適用率
システム運用	ポリシーに準拠した ID 管理の適用数と適用率
セキュリティ監査	バッチ管理の適用数と適用率
	ぜい弱性診断の診断回数とぜい弱性の発見数
	監査回数と指摘事項数
セキュリティ事故	不正アクセス、ウイルス感染等の事故件数と復旧までの時間（RTO）
	個人情報流出事象の発生件数と影響規模

この他、NIST SP800-55（Security Metrics Guide for Information Technology Systems：情報技術システムのためのセキュリティメトリクスガイド）[30]には FISMA ベースの情報セキュリティ効果測定指標がまとめられている。また、ISO/IEC JTC1[31]において、ISO/IEC 27001:2005 のフレームワークに基づく測定の手法と測定例についての国際標準 ISO/IEC 27004（ISM Metrics and Measurements：管理策の評価指標及び測定のためのガイドライン）の検討が進められている。

4.2.2. 測定の可視化

前述のように、組織内にある測定可能な指標は膨大な数になるため、指標を測定するにあたっては測定の適切な計画と設計が不可欠である。

まず、どのような測定手法を使うかを検討する。インタビューや監査は数値化されない定性的な情報を集めるのに適した手法である。このとき、チェックシートなどを利用することにより、ある程度の客観性を持った測定を行うこともできる。インタビューや監査は自動化した測定に比べ初期コストが低いので、情報収集の期間が長い場合や、情報収集対象や測定方法が頻繁に変化する場合にも有利な手法になる。表 4-3 は実際に企業で使用されているモニタリング指標収集のためのチェックシートの例である。

[30] http://csrc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf
[31] ISO と IEC の合同専門委員会 1(Joint Technical Committee 1)。情報技術に関する標準化活動を行う。

表 4-3 モニタリング指標収集のためのチェックシート例（部分）

管理策	有効性測定の項目／評価基準	達成基準
情報セキュリティ 基本方針	1.「セキュリティ基本方針」を確認 （1）事務所における掲示確認。責任者に周知し理解している。 （2）事務所における掲示確認。責任者の一部が理解不足である。 （3）事務所での掲示確認できず。または責任者の理解不足多数。	（1）
第三者との契約に おけるセキュリティ	2. 業務委託先との契約関連書類を確認 （1）「受託者用情報管理要綱」を十分理解している。 （2）文書の存在は認識しているが、内容に精通していない。 （3）文書の存在、内容、共に理解していない。	（1）
資産目録	3. パソコンの増減管理状況の確認 （1）保有パソコンを管理台帳に登録済み。 （2）一部の未登録パソコンを確認した。 （3）未登録パソコンの存在確認を実施していない。	（1）
資産の管理責任者	4. パソコンセキュリティ点検の確認 （1）保有パソコンの点検状況を確認し、不備について改善指示中。 （2）保有パソコンの点検状況を確認したが、不備について指摘をしていない。 （3）保有パソコンの点検情報を確認していない。	（1）
情報のラベル付け 及び取扱い	5. 情報管理規定による情報の格付け状況を確認 （1）格付けとして「社外秘」「関係者外秘」「厳秘」を表示している。 （2）一部のファイルに格付けが行われていない。 （3）多くのファイルに格付けが行われていない。	（1）

内部監査の仕組みを活用して、モニタリング指標を調査することも可能である。非監査部門から独立した経営者直轄の機能である内部監査は、業務プロセスや資産、体制、経営環境等の知見を有するため、マネジメントシステムの有効性を評価するのに適している。特に、情報セキュリティ管理策の有効性評価には、情報セキュリティ監査が有用である。

各種の機器で発生するログやイベントメッセージなども測定の対象となり得る。これらは一度収集の仕組みを構築してしまえば低いコストで定常的に情報を収集することができるが、一般に有用な情報が大量の情報に埋まってしまうことが多く、意味のある情報を取り出すために加工が必要となる。

組織内で発生するインシデントも測定の対象とするべきである。インシデントは、その拡大を防止し適切な対処を実施するために、観測されたらただちに関係する部門・要員などに通報されるように監視の体制と仕組みを組織内に構築する必要がある。また、インシデントの発生実績は情報セキュリティ対策の有効性を判断するために不可欠の情報であり、

確実に収集して活用するべきである。

インターネットサーバなど直接攻撃の対象となりやすい機器については、ぜい弱性やリスクの有無を直接測定すると効果的である。専門的知識を持ったセキュリティエンジニアによる侵入テストの結果報告、ぜい弱性スキャナの測定レポート、侵入検知システム（IDS）や侵入防御システム（IPS）の検知情報などを測定値として利用することができる。

測定値をシステムなどで自動的に収集する場合は、効率的に情報を収集・処理するための検討が必要になる。例えば、運用管理ミドルウェアのような、組織内に広く存在する各種の機器から情報を集めるためのソフトウェアを利用することも有効である。

また、収集した事項をできるかぎり直感的に把握できるように提示するために、例えば、一つの画面でその状況を網羅的に把握できるように配置したダッシュボードのような形が考えられる（付録 4 参照）。

4.3. モニタリングで把握する内容と対応するモニタリング指標の例

モニタリングで把握すべき事項には、経営陣、CISO、管理者それぞれが単独で測定可能な事項もあるが、多くは互いに連携することで測定可能となると考えられる。例えば、情報セキュリティ投資効果として「情報セキュリティ推進体制が適切に運営されているかどうか」についてモニタリングを行うことを経営陣が決定し CISO に対して指示を行ったとすると、CISO は上記目的の達成度を測定するための情報セキュリティ目的・目標を複数設定することになる。

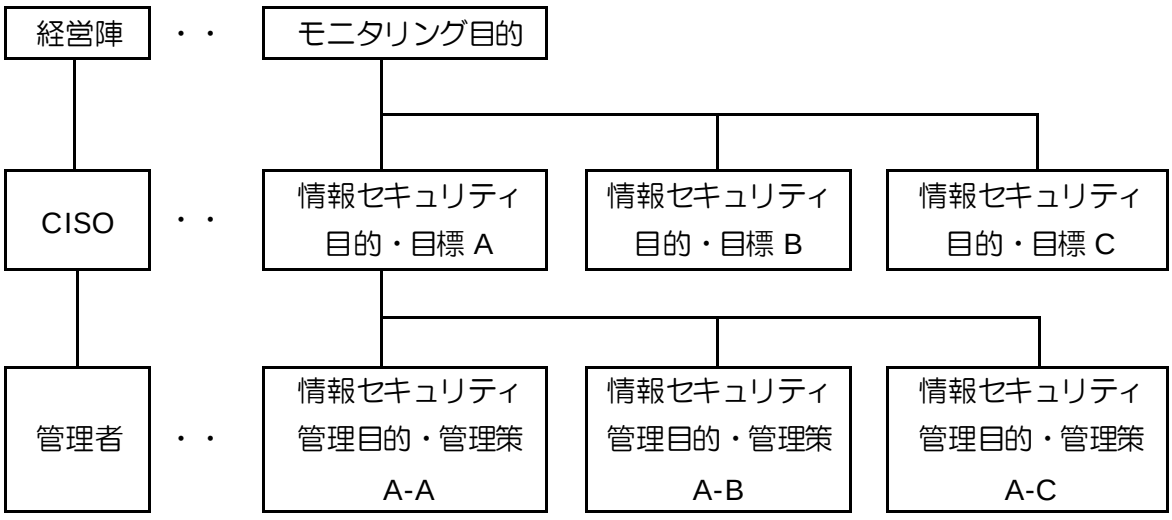


図 4-2 各階層におけるモニタリング指標の関係

また、経営陣、CISO は一つのユニットとして存在するが、管理者は部門、部署ごとに存在するため、各管理者において異なる情報セキュリティ管理策を持ち、異なるモニタリング指標を持つことになる。あるいは、同じ情報セキュリティ管理策であっても、部門、部

署の性格、構造の違い等により、異なるモニタリング指標が導き出されることも考えられる。

経営陣、CISO、各管理者は、このような階層関係が構築されていることに常に配慮し、経営陣あるいは CISO はモニタリング全体構造として整合性がとれていることを定期的に検証する必要がある。

4.3.1. 経営陣の場合

経営陣が行うモニタリングは、例えば、経営環境、情報セキュリティ投資効果、情報セキュリティ目的・目標達成度評価等の項目が考えられる。ただし、経営陣が検討しなければならないリスクの分野は情報セキュリティ分野にとどまらず広範なため、複数の分野に共通する項目（経営環境）や集約された項目（CISO からの報告）が中心となる。

表 4-4 経営陣が行うモニタリングの例

項目	モニタリング内容の例	指標例
経営環境	・市場環境に変化はあるか ・関連の法令制度に変更はあるか ・経営資源の状況に変化はあるか （例：不況による予算抑制等） ・競合状況に変化はあるか ・技術、インフラに変化はあるか	・顧客属性推移 ・売上推移 ・法令改正への対応の有無 ・IT 投資計画 ・競合他社動向
情報セキュリティ投資効果	・情報セキュリティ推進体制が適切に運営されているか ・リスク分析の結果に照らして情報セキュリティ投資は効率的かつ効果的か ・インシデント件数及び被害を低減できているか ・情報セキュリティに関する法令遵守の徹底	・CISO による報告（詳細は表 4-5 参照）
情報セキュリティ目的・目標達成度評価	・リスク管理方針に則り、CISO が設定した情報セキュリティ目的・目標が達成できたか	・CISO による報告（詳細は 5.2 節参照）

特に、CISO は、集約した結果をそのまま報告するのではなく、そこから重要なメッセージのみを抽出し、経営陣に対し的確に理解できるよう昇華した内容を報告する必要がある。

4.3.2. CISO の場合

CISO が行うモニタリングは、例えば、情報セキュリティ投資効果、情報セキュリティ目標の達成状況、PDCA の進捗・達成状況等が考えられる。情報セキュリティ目標を 4.3.1 節で例示した内容で設定した場合の、モニタリング内容とモニタリング指標の例を表 4-5 に

示す。

表 4-5 CISO が行うモニタリングの例

項目	モニタリング内容の例	指標例
情報セキュリティ投資効果	・情報セキュリティ推進体制 ・セキュリティ方針策定と承認が適切にされているか ・定期的にセキュリティ委員会が開催され課題が共有されているか ・部門管理責任者とその担当範囲は適切か	・委員会議事録 ・担当範囲の見直し記録
	・情報セキュリティ投資 ・投資の効率は審議されているか ・新規の管理策：投資対効果が検討されたか ・継続の管理策：効率化が図られているか ・リスク管理方針に照らして投資の対象や内容は妥当か	・管理策選定議事録 ・効率化プロセス数、割合 ・削減額 ・リスク管理方針に照らしたレビュー頻度
	・インシデント件数及び被害の実質的な低減[32] ・インシデント報告件数は減少しているか ・インシデントの被害額は減少しているか ・インシデントの報告と対応は適正になされているか ・インシデントの再発防止策が検討・実施されているか ・インシデントの解決率は向上しているか ・インシデント対応への初動時間は短縮しているか	・報告記録 ・対応計画の進捗報告 ・内部監査記録 ・報告記録
	・法令遵守の徹底 ・法制度や業界標準への対応がなされているか ・情報セキュリティに関する法令違反が発生したか	

[32]発生したインシデント・被害の検出率を 100%に近づける努力を行い、その成果が十分に現れた上で初めて、件数・被害の低減が意味のある指標となる。

情報セキュリティ目標の達成状況	・他社との共有資産である技術情報を含む重要情報が明確に区分され、会社の定める規程に則り適切に管理されているか ・情報管理規程が遵守されているか ・持ち出し PC 上の情報管理 ・協力会社との機密保持契約締結 ・情報システムの停止や処理能力の著しい低下が発生した場合にも、最低限の生産体制が維持できるよう、適切かつ合理的な方策が適用されているか ・製造ラインの IT 汎用技術導入に応じて適切な情報セキュリティ管理策を適用しているか	・情報資産管理台帳整備率 ・内部監査記録 ・規程違反数 ・PC セキュリティ設定遵守率 ・NDA 締結率 ・事業継続訓練実施回数 ・事故時のサービス停止時間 ・対象のリスク分析結果 ・対応計画の進捗報告
PDCA の進捗・達成状況	・セキュリティマネジメントの進捗状況は適正か（計画、管理策適用、監査などの進捗状況） ・重要な情報資産の区分と管理は適正か ・情報セキュリティ教育の実施状況は適正か ・管理策の有効性は確認できたか ・その他、顕在化した問題について、適正な改善がなされているか	・各部門からの報告数、実施率、所要日数

4.3.3. 管理者の場合

各部門における情報セキュリティの管理者は、情報セキュリティ管理目的・管理策の有効性を評価するために、情報セキュリティ管理目的・管理策の適用状況を把握する必要がある。その際、総合的な指標よりもむしろ現場で起こった問題点をより早く伝達し、また正しい対処を行うためにできるだけ正確な情報を直接提供することが求められる。現場の管理職・担当者においても同様な傾向がある。

表 4-6 管理者が行うモニタリングの例

項目	モニタリング内容	指標例
セキュリティマネジメントの進捗状況	・情報セキュリティマネジメント計画の進捗状況 ・情報セキュリティ管理策の適用状況 ・情報セキュリティ監査の実施状況	・進捗率 ・適用率 ・実施率
情報資産の管理	・情報資産の識別状況 ・情報資産の管理状況	・識別率 ・管理率
情報セキュリティ教育の実	・情報セキュリティ教育の受講状況 ・情報セキュリティ教育の実施効果	・受講率 ・成績向上率

施		
情報セキュリティ管理策の有効性評価	・システム開発・構築時のセキュリティ向上 ・システム運用におけるセキュリティ向上	・事件・事故発生件数

各管理者は、モニタリング項目について CISO から指示を受け、担当する部門、部署に適合したモニタリング内容、指標を設定することになる。

【ISMS と他のマネジメントシステム、制度等との融合】

情報セキュリティマネジメント（ISMS）規格 ISO/IEC 27001:2005 の認証を取得する際、すでに品質マネジメントシステム（QMS）規格（ISO 9001:2000）や環境マネジメントシステム（EMS）規格（ISO 14001:2004）の認証を取得している場合、それらの関係をどのように整理すべきかが問題となるケースが見られる。また、特定の部門で ISMS 認証を取得し、その後全社に拡大していく過程で、既存のルール・体制との整合性に悩み始める企業も少なくない。さらに最近では、金融商品取引法に基づく内部統制報告制度の導入に伴い、同制度と ISMS をどのように整理すればよいのか悩む場合もある。認証規格の項目の異同で悩むことも多い。

本来、ISMS も内部統制の一部であり、企業のガバナンスや内部統制が適切であれば、他の規格や制度との整合性に悩む必要はない。全体の内部統制を無視して、情報セキュリティの部分だけ ISMS の認証規格にあわせて組織作りをしようとすると、制度間の異同や認証規格の項目の異同が問題になる。また、一部の部門だけで ISMS の認証規格にあわせて組織作りをしようとしても、認証範囲の拡大や他の制度との調整が必要となったときに整合性がとれなくなる。企業全体としてのガバナンスや内部統制を重視し、それと整合をとる形で ISMS 認証等の制度を活用することが肝要である。

5. 評価

本章では、「モニタリング（Monitor）」で得た情報を踏まえ、「方向付け（Direct）」の妥当性を「評価（Evaluate）」する仕組みについて解説する。

評価とは、得られた材料を持って、想定していた仮説について検証する作業である。評価の結果、見直しが必要と判断された場合には、方向付け（Direct）の活動にフィードバックされ、修正された新たな方向を指し示すことになる。

5.1. 経営陣が行う評価

経営陣は、モニタリングから得られた情報を踏まえ、自らが提示したリスク管理方針の妥当性を評価する。経営陣が行うべき評価の視点は、以下のようになる。

(1) 経営環境の変化に対応できるか

経営環境の変化から、リスクの変動や新規リスクの発生が明らかになった場合、リスク管理方針の前提条件が変化したと捉え、現在のリスク管理方針がそうした変化に対応できるかどうかを評価する。例えば、ネット販売を始めたところ、ユーザのネット経由の購入割合が急増して、ユーザの個人情報やクレジットカード番号等の重要情報が当初想定より大幅に増えた場合、Web サイトが抱えるリスクは増大していることから、現在の許容リスク水準を維持して対策を強化するのか、予算との兼ね合いで許容リスク水準を見直しつつ既存の対策で対応するのかは経営判断である。

(2)リスク管理方針が適切か

リスク管理方針そのものが適切であったかどうか、明示した許容リスク水準に基づき行われた情報セキュリティに関する経営資源の投入が投資対効果の観点から適切かどうかを評価する。具体的には、推進体制の活動状況、投資の効率性、インシデントや法令違反の発生状況（投資の有効性）などのモニタリング結果から、許容リスク水準やそれに基づく経営資源の投入に関する判断の妥当性を評価する。

(3)リスク管理方針が適切に実装できているか

情報セキュリティ目的・目標がリスク管理方針に基づき策定されたものであることから、情報セキュリティ目的・目標の達成状況がリスク管理方針の実装状況と捉えることができる。特に、PDCA が適切に実施されることにより、リスク管理方針が適切に維持されることにつながる。

これらの観点に基づく評価結果を踏まえ、経営陣はリスク管理方針の見直しの必要性を検討し、必要に応じて、リスク管理方針の改訂を行う（Direct）。

5.2. CISO が行う評価

CISO は、モニタリングから得られた情報を踏まえ、リスク管理方針に則り策定した情報セキュリティ目的・目標の達成度を評価する。CISO が行うべき評価の視点は、以下のようになる。

(1)情報セキュリティ目標が達成できたか

CISO は、モニタリングの結果を踏まえ、設定した個々の情報セキュリティ目標が達成できたかどうかを評価する。それぞれ KPI[33]や KGI[34]として捉えた際の、想定した水準に達しているかが判断基準となる。例えば、「すべての PC についてセキュリティ設定を遵守すること」を目標としていたが、点検の結果、遵守率 98%となった場合、それを「未達」とするか、改善を促す条件付で「達成」とするかは、CISO の判断である。

(2)情報セキュリティ目的が達成できたか

情報セキュリティ目的の達成度は、情報セキュリティ目標の達成度から評価する。関連する目標の達成度の積み重ねをどのように評価するかは、情報セキュリティ目的の趣旨に照らし合わせて CISO が判断するポイントである。

また、場合によっては、外注先や外部委託先など組織外部を含めた形で評価を行わなければならない可能性もある。このような場合に備えて、このようなアウトソース先を巻き込んだ情報セキュリティガバナンスの確立と維持についても検討しておく必要があると考えられる。

アウトソース先から入手する情報としては、以下の項目等が挙げられる。

- 個人情報などの情報資産の取扱規程の遵守状況
- アクセスコントロールや暗号などのセキュリティ対策の状況
- 重要情報の取扱者の明確化とそのアクセス履歴及び廃棄状況
- セキュリティ事故やインシデントの状況

[33] Key Performance Indicator
[34] Key Goal Indicator

6. 監督

企業における情報セキュリティガバナンスの確立を自律的に進展させるメカニズムとして、株式市場をはじめとする社外利害関係者の評価と、経営陣の活動を「監督（Oversee）」、すなわち問題点を指摘し改善を求める監査等の取組がある。前者は時間をかけて形成する必要があるのに対し、監査は既存のフレームを活用することができる。

経営陣に対する監視機能として、我が国の監査役制度は独特の歴史的な経過をたどり、諸外国[35]にはほとんどその例を見ないものとして存在している。2002 年の商法改正により、企業は監査役会設置会社から委員会等設置会社への移行が可能になったが、現在も監査役制度を維持する企業が大多数を占めていることを踏まえ、本章では、我が国の監査役制度下の対応を中心に説明する。

6.1. 監査役監査による対応

監査役監査は、取締役から独立した立場から取締役の職務執行を対象とする点で、情報セキュリティガバナンスのフレームワークに基づく経営陣の活動の有効性を検証するのに適している。

監査役監査は、取締役の行う業務執行を対象として行う業務監査と、会計記録や会計処理業務を対象として行う会計監査で構成される。情報セキュリティガバナンスについては、業務監査の一つである「内部統制システムに係る監査」の一環として扱うことが適当である。

内部統制システムに係る監査は、会社法（362 条 4 項 6 号、416 条 1 項 1 号ロ及びホ、会社法施行規則 100 条 1 項及び 3 項、112 条）等に基づき、監査役に求められているもので、社団法人日本監査役協会が制定した監査役監査基準によると、監査役は会社の取締役会決議に基づいて整備された内部統制システムの内容、整備･運用状況を監視・検証する必要がある（監査役監査基準 21 条 1 項）。監査役は、内部統制システムの構築及び運用の状況についての報告を取締役に対し定期的に求めるほか、内部監査部門等との連係及び会計監査人からの報告等を通じて、内部統制システムの状況を監視し検証することが求められる。不十分な内部統制システムについて監査不備があれば、監査役は善管注意義務違反となる可能性に留意しなければならない。

また、内部統制システムに関するより具体的な監査の方法等については、「内部統制システムに係る監査の実施基準」として制定されている。

同実施基準では、「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

[35]欧米の場合、経営の執行は CEO を頂点とする Executive（執行役）が担い、それを Board（取締役会）の Director（取締役）が監督することで、経営の執行と監督機能の分離を実現している。

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」や「重要な営業秘密、ノウハウ、機密情報や、個人情報ほか法令上保存・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」について、統制の有無を確認することを監査役に求めている。

こうした内部統制に係る監査業務については、取組の一環として、情報セキュリティガバナンスに係る監査、すなわち「方向付け（Direct）」、「モニタリング（Monitor）」、「評価（Evaluate）」といった経営陣の活動の監査をカバーすることは可能と考えられる。

表 6-1 情報セキュリティガバナンスの活動に係る監査の要点（例）

活動項目	確認すべき点の例
方向付け （Direct）	・リスク管理方針が適切な手順を経て策定されたか ・リスク管理方針が経営戦略を反映しているか ・経営陣はリスクを理解しているか ・CISO からの展開が適切に行われたか
モニタリング （Monitor）	・経営陣及び CISO が正確に状況を把握できるようにモニタリングの体制や仕組みが整備され、稼動しているか
評価 （Evaluate）	・モニタリングで得られた情報が評価に反映されているか ・評価結果を方向付けの見直しに反映できているか

6.2. 内部監査との連携

内部監査は、業務の執行部門から独立した立場の社内リソースが、業務執行の戦略・目標に関する達成状況、取組、課題などをモニタリングする機能である。企業自らが実施する内部監査の仕組みを活用すれば、リスク管理上の問題に早い段階から対処することができる。非監査部門から独立した経営者直轄の機能である内部監査は、業務プロセスや資産、体制、経営環境等の知見を有するため、マネジメントシステムの有効性を評価するのに適している。実務上は、情報セキュリティ監査の適用が効率的である。

監査役監査と内部監査の関係は、以下に示すとおり、情報セキュリティガバナンスを監査役監査が、情報セキュリティマネジメントを内部監査がカバーする構成となる。

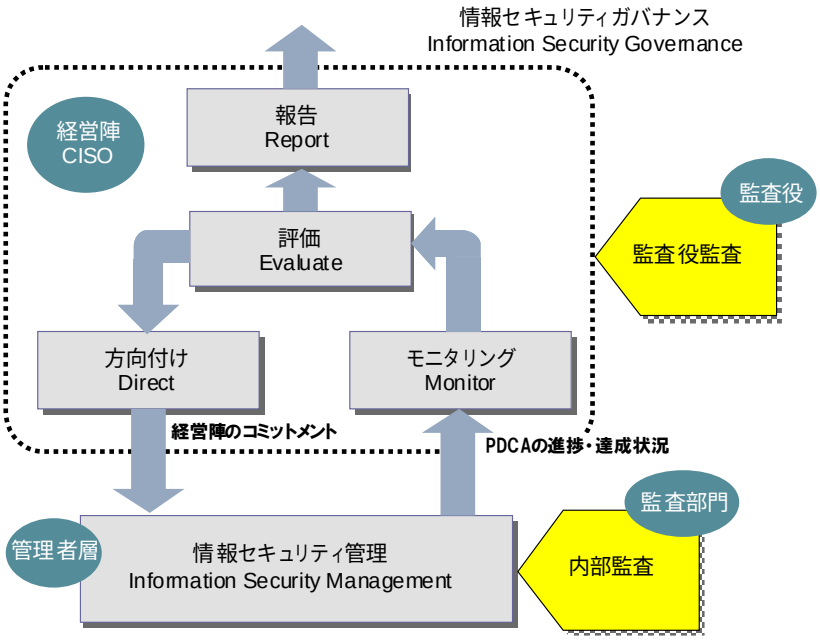


図 6-1 情報セキュリティ分野における監査役監査、内部監査の位置付け

内部監査で得られた情報は、監査役監査実施する上で有効に活用できる。そこで、社団法人日本監査役協会「内部統制システムに係る監査の実施基準」でも、監査役は内部監査部門等との連携が実効的に行われるよう要請することができる。（第 16 条）

なお、経営者の指揮下にある内部監査部門スタッフが経営者の職務遂行を監査する監査役スタッフを兼務する場合には、その業務範囲や責任、権限等を社内規程で明確にしておくことが望ましい。

7. 情報セキュリティに関する報告

7.1. アカウンタビリティと価値創造

自社が情報セキュリティに関わる取組を実践していることを社内外の利害関係者に認知させることには 2 つの狙いがある。

一つは、社会から期待されている取組を実践していることを報告することで、企業が社会的責任を果たしていることを表明するという狙いが考えられる。情報セキュリティに関する事件・事故の発生は、取引先や顧客に重大な影響を与え、さらに場合によっては自社のシステムを悪用されて、自覚なく不正行為の一端を担い、ネット社会全体にも迷惑を及ぼす加害者となることもある。にもかかわらず、社外の利害関係者には、各社がどれほど積極的に情報セキュリティに関わる取組に熱心であるのかが確認できない。こうした社外利害関係者の不安感や不信感を発生させないという観点から、企業の社会的責任として、情報セキュリティに関わる取組を報告するのである。

かつては、情報セキュリティに関する事件・事故もそれほど頻繁ではなく、情報セキュリティに熱心ではない企業であっても、従来は大きな問題とならないことが多く、信頼を得ることが可能であった。しかしながら近年、個人情報の流出やシステム障害によるサービス停止の多発により、例え情報セキュリティの取組を積極的に実施している企業であっても、社外の利害関係者はそれを把握することができず、事件・事故が発生した企業と同様のリスクを抱えていると見なす可能性もある。したがって「アカウンタビリティ」の観点から、情報セキュリティに関わる取組を開示することで、そうしたネガティブな評判の発生を避け、社外の利害関係者を安心させる必要がある。

一つは、企業価値を高めるという観点から、情報セキュリティに関わる取組を報告するという狙いが考えられる。情報セキュリティに対する取組は、取引先や顧客の信頼感を増幅させ、結果として取引先との安定的な関係の構築や顧客からのロイヤリティやプレミアム、あるいは情報資産の戦略的な管理に結びつけば、企業の将来キャッシュ・フローの増大ないしは安定化することが可能となる。しかしながらこうした経済効果は、企業サイドから開示しない限り、投資家などからの評価には結びつくことはまれであろう。

二つの狙いは相互排他的であるとは限らない。また情報セキュリティに関する取組を開示することは、そこで働く社員の情報セキュリティに対する意識や自覚を高める副次的な効果も期待できるという意味で重要である。社外に対する報告、すなわち「開示」は、企業が社会に対して説明している「約束」と位置付けることも可能である。企業としての取組を開示することで、社員一人ひとりにその「約束」を徹底させることの重要性を強調することもできるためである。

7.2. 法定開示と自発的開示

情報セキュリティに関わる取組を開示する場合、2つの開示アプローチを想定することが可能である。

一つは、法定開示の中で取組内容を開示することができる。例えば、金融商品取引法が開示を要求している有価証券報告書の中では、近年、「対処すべき課題」「事業等のリスク」「コーポレートガバナンスの状況」など定性情報の拡充が進展している。また金融機関が開示を求められるディスクロージャー誌においては、「リスク管理の体制」を開示することが求められている。このように新たに開示されるようになったこれらの項目で共通しているのは、企業ごとに取組内容などが多様であり、統一的な開示基準を作ることは適当でないという点であり、このため、各社の実態に即した開示を実践することが望ましい。情報セキュリティに関する取組についても、これらの開示チャネルを通じて開示している企業も多い。

もう一つは、情報セキュリティ報告書や CSR 報告書、防災報告書など自発的な開示チャネルを活用し、開示するアプローチがあり得る。近年、会計研究において、貸借対照表や損益計算書に計上される情報と株価に代表される企業価値の統計的な関連性が弱くなっていることを示唆する検証結果が相次ぎ公表されつつある。こうした結果を受けて、企業の特定の活動を自発的な開示チャネルを通じて開示するケースが相次いでいる。こうした中で、情報セキュリティに関する取組を独自の報告書を作成し、開示するケースも見られる。さらに、ISMS やプライバシーマーク、情報セキュリティ格付など、開示アプローチの選択肢が充実しつつある。

7.3. 情報セキュリティ開示の対象と内容

情報セキュリティの開示先として、想定できる利害関係者は、株主、債権者、顧客、取引先、アウトソーシング先等である。

まず、株主や債権者など企業に対する資金提供者を挙げることができる。情報セキュリティに関わる取組は、財務報告の信頼性を高める上での重要プロセスと位置付けられていることは、昨今の内部統制の構築をめぐる一連の議論の中でも強く意識されている。また会社法で取締役にその構築を求めている内部統制においても、情報の保有ならびに管理に関する体制や損失の危機の管理に関する規程その他の体制、使用人の職務の執行が法令及び定款に適合するための体制など、情報セキュリティに関わる取組と深く関わる体制の整備が求められることが確認できる。企業がより多様で深刻なリスクにさらされるケースが多くなる中で、株主や債権者など企業の資金提供者にとって、内部統制に関する情報の重要性が飛躍的に増大しており、その主要な取組としての情報セキュリティに関する情報も重要になりつつあると推測することができる。

また、顧客や取引先、アウトソーシング先も、想定される開示先に挙げることができる。技術やノウハウなどの機密情報や顧客情報、情報ネットワークの戦略的な重要性が高まる中で、その共有と管理をいかに進めるべきかが重要な経営テーマとなりつつある。こうした情報資産を戦略的に活用していくためには、その漏えいや流出を防ぐ仕組みとしての情報セキュリティについての取組を開示・説明していくことが重要となるのである。

また、情報セキュリティの取組を開示するとした場合、その狙いに応じて、開示すべき内容は異なる。

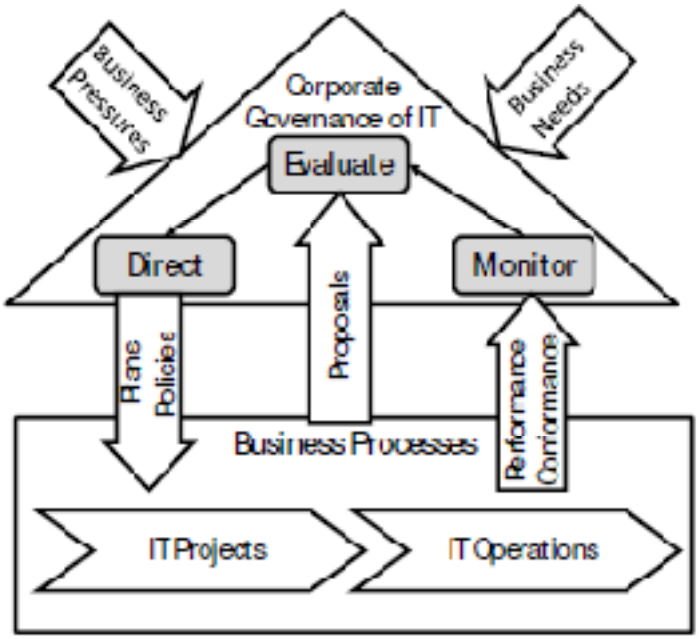
「アカウンタビリティ」の観点から開示する場合には、社会が期待する情報セキュリティの取組が実践できているかどうかについて判断できる材料を提供することが重要である。ここで重要となるのは、どのような情報セキュリティポリシーを掲げており、当該ポリシーをどのようなプロセスで実践しようとしているのか、その実効性を担保するのはどのような体制であるのか、という点を判断できる情報と考えられる。このため、開示すべき内容は、①情報セキュリティポリシー、②リスク評価、③リスク対応、取組内容、④実施体制などが重要となると考えられる。

一方、「価値創造」の観点から開示する場合、重要となるのは、それがどのような経済効果を生み出しているのかという点である。情報セキュリティに関わる取組が情報資産の棚卸などを経てどれほどのコスト削減に結びついているのか、あるいは情報セキュリティに関わる取組が顧客や取引先に対する信頼感の醸成などブランド価値にどれほど結びついているのか、情報セキュリティに関わる取組を通じて守っている情報資産がどれほどの経済価値を持ち、情報セキュリティに関わる取組を実践することで、その喪失の可能性をどれほど低下させているのか、などの経済効果を確認できれば、投資家などの資金提供者は当該企業の企業価値を高く見積もることとなり、当該企業の株式市場からの評価などを高めることに結びつく。

付録1.ISO/IEC 38500:2008 のモデル

ISO/IEC 38500:2008（Corporate governance of information technology）は、企業の IT ガバナンスに関する国際標準として 2008 年 6 月に規格化された。ISO/IEC 38500:2008 において提唱されているモデル（下図）では、「Direct」「Evaluate」「Monitor」の 3 つのタスクを通じて、Director が IT ガバナンスを行うことを推奨している。

- 現状及び将来の IT 活用を評価する（Evaluate）
- ビジネス活動に適合した IT 活用を勧めるための計画やポリシーを準備し実装するために方向付けする（Direct）
- ポリシーやパフォーマンスが計画と合致していることをモニタリングする（Monitor）



Model for Corporate Governance of IT

（出典：ISO/IEC 38500:2008(Corporate Governance of Information Technology)）

付録2.会社法が求めるITに関する統制の全体像

【 会社法での要求事項 】

本節は、情報セキュリティガバナンス研究会/情報セキュリティ関連法律上の要求事項検討ワーキンググループ「情報セキュリティ関連法令の要求事項集」より一部概要を紹介する 。

内部統制とは「会社が営む事業の規模、特性等に応じたリスク管理体制」と定義される。取締役には、会社に対する善管注意義務（会社法第330条、民法第644条）に基づいて、このような内部統制に関する基本方針を取締役会で決定し、決定した基本方針に従った内部統制を構築する義務がある。

会社法は、大会社と委員会設置会社について、内部統制システムの構築の基本方針を取締役会で決定すべきことを明文の義務としている（会社法第348条第3項第4号、第362条第4項第6号、第416条第1項第1号ホ）。これらの規定は、善管注意義務から要求される内部統制システム構築の基本方針決定義務を念のために明文にしたものである。決定すべき内部統制は、類型に分けて列挙されている。その中には、①法令等遵守体制、②損失危険管理体制、③情報保存管理体制、④効率性確保体制、⑤企業集団内部統制が含まれる（前記引用の会社法各条及び会社法施行規則第98条第1項、第2項、第100条第1項、第112条第1項、第2項）。情報セキュリティに関するリスクが、会社に重大な損失をもたらす危険のある場合には、②の損失危険管理体制（損失の危険の管理に関する規程その他の体制をいう）に含まれる。

会社法は、「業務の適正を確保するための体制の整備」について取締役会が決すべきものとしているが、当該体制の具体的な在り方は、一義的に定まるものではなく、各会社が営む事業の規模や特性等に応じて、その必要性、効果、実施のためのコスト等様々な事情を勘案の上、各会社において決定されるべき事項である。また、取締役会が決めるのは「目標の設定、目標達成のために必要な内部組織及び権限、内部組織間の連絡方法、是正すべき事実が生じた場合の是正方法等に関する重要な事項（要綱・大綱）[36]」でよいと解されている。

【 IT統制の対応 】

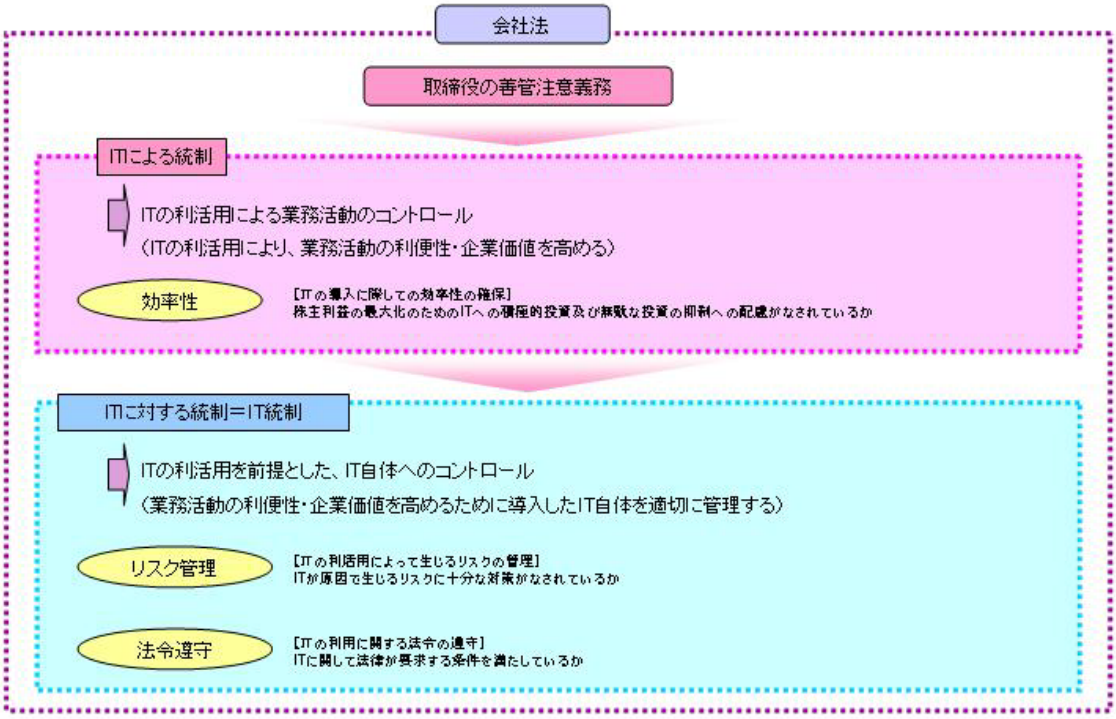
そもそもITに関する統制の内容に関しては様々な考え方があり、一義的に定まった理解を確立することは難しいが、会社法に定められる取締役の善管注意義務の観点からは、以下の3段階に分けて考えることが適当であると考えられる。

すなわち、まず、取締役は会社から委任を受けて経営を行っているため、善管注意義務

[36] 相澤哲ほか『論点解説新・会社法』335頁

の観点から、株主利益の最大化のために企業活動の効率性を確保することが必要となり、このような効率性確保の目的で IT の利活用を行うことが考えられる(①「IT による統制」)。この場合、IT 導入に際しての投資対効果等にも配慮する必要がある。

次に、このように IT を利活用する場合には、取締役の善管注意義務の観点から適正な経営を行う必要があり、IT 自体を適切に管理することが求められる(「IT に対する統制」(=「IT 統制」)。IT に対する統制はその目的によって 2 つに分けられ、②IT に関するリスク管理を目的とした IT に対する統制、更に、③システムや情報の種類等により一定の IT に対する統制が法令で要求されている場合は、IT に関する法令遵守を目的とした IT に対する統制、が考えられる。

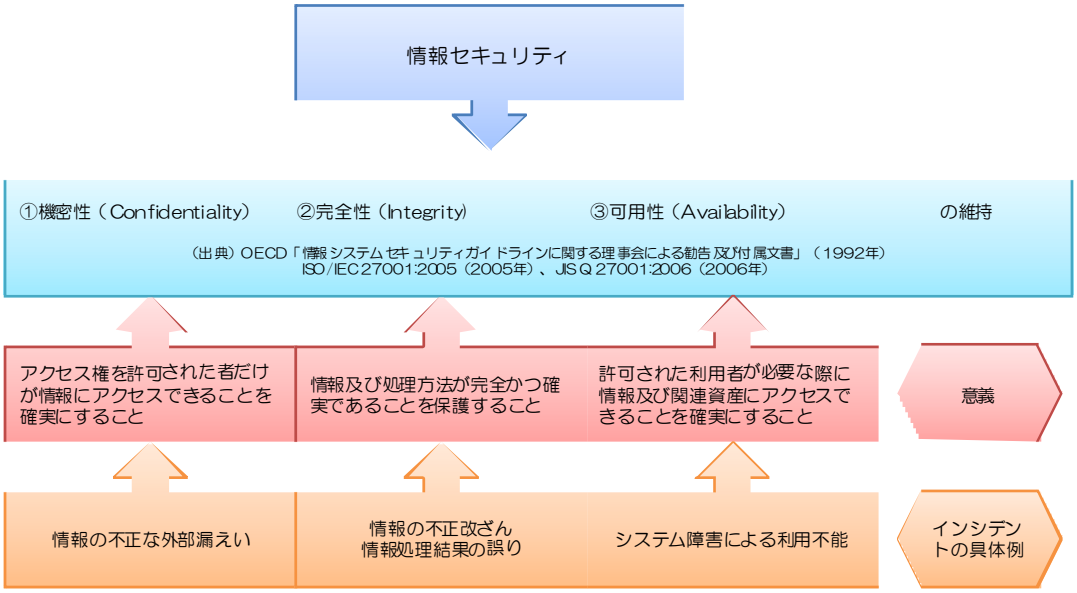


(出典)情報通信総合研究所作成

IT 統制の考え方

IT に対する統制の内容としては、システムの停止や、機密情報・個人情報の漏洩等、様々な IT リスクへの対応が中心となるものと考えられるが、こうした対応の一つとして企業活動に欠かすことができないものとして、情報セキュリティ対策を挙げることができよう。情報セキュリティとは、機密性(Confidentiality)、完全性(Integrity)、可用性(Availability)を維持することであり、システム障害による利用不能や情報の不正改竄、情報漏洩等を防止するために重要な機能を担うものであると言える。

そして、先に述べたようなシステム障害事例や情報漏洩事例等が頻発し、企業活動に付随する IT リスクが高まっている現状に鑑みれば、会社法の定める善管注意義務から導かれる IT に対する統制の一環として、取締役会においてセキュリティポリシーの策定等を行い、それに基づいて企業の情報セキュリティ対策を進めていくことが、望ましいと考えられる。また、各企業において、それぞれ業種及び規模等に応じてある程度具体的なセキュリティポリシーを定めることが望ましい。



岡村 久道「情報セキュリティの法律」（商事法務、2007年、3頁）より情報通信総合研究所が作成した図を一部修正

機密性・完全性・可用性の維持

もっとも、取締役の善管注意義務を IT に関する統制の根拠として基礎付けると解したとしても、取締役には経営判断の原則が認められるため、当該状況下で事実認識・意思決定過程に不注意がなければ、取締役には広い裁量の余地が認められると解されており、取締役の法的責任が問われるのは、限られた場面に過ぎないことには留意が必要である。すなわち、会社法の善管注意義務が要求する最低限のミニマムスタンダードと、更に望ましいレベルでのベストプラクティスは、厳密にはレベルの異なる問題なのであり、両者の違いを踏まえ、どの程度の統制を行えば善管注意義務違反にならないのかという分水嶺をある程度明確化することが、企業が実際に IT に関する統制を構築していくにあたって有益であろう。こうした問題については、今後の課題として検討していくことが必要と考えられる。

付録3.内部統制システムに係る監査の実施基準（抜粋）

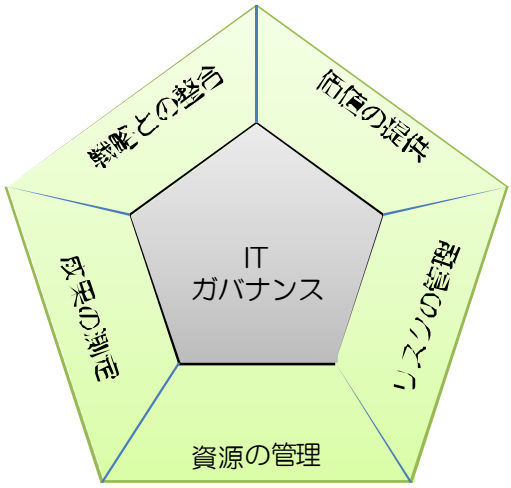
社団法人 日本監査役協会「内部統制システムに係る監査の実施基準」（2007/04/05 制定）より、「損失危険管理体制の監査」「情報保存管理体制に関する監査」の記述を抜粋し、下表にまとめる。

基準	監査上の重要な着眼点	重要な統制上の要点
第9条 損失危険管理体制に関する監査	・損失の危険の適正な管理に必要な諸要因の事前の識別・分析・評価・対応に重大な漏れ・誤りがあった結果、会社に著しい損害が生じるリスク ・会社に著しい損害を及ぼすおそれのある事業活動が正当な理由なく継続されるリスク ・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	・代表取締役等が、会社経営において損失危険管理及びその実効的体制の整備が必要不可欠であることを認識しているか ・会社に著しい損害を及ぼすおそれのある事象への対応について、取締役会その他重要な会議等において、十分な情報を踏まえたリスク分析を経た議論がなされているか ・代表取締役等が、会社の事業内容ごとに、信用・ブランドの毀損その他会社存続にかかわるリスクを認識しているか。当該リスクの発生可能性及びリスク発生時の損害の大きさに関する適正な評価が行われているか。他社における事故事例の把握、安全・環境に対する社会的価値観の変化、法的規制その他経営環境及びリスク要因の変化が認識され、それに対して適時かつ適切に対応する体制が整備されているか ・当該事業年度において重点的に取り組むべきリスク対応計画を策定しているか。当該計画の実行状況が定期的にレビューされる仕組みが整備されているか ・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ているか。定められた規程及び職務分掌に従った業務が実施されているか。損失危険管理の状況を監視するモニタリング部門が存在し、会社の損失危険管理に係る問題点が発見され、改善措置が講じられているか ・会社に著しい損害を及ぼすおそれのある事業活動の継続に関し、適時かつ適切な検討が行われているか。正当な理由なく放置されていないか ・損失危険管理体制の実効性に重要な影響を及ぼしうる事項について、取締役会及び監査役に対して定期的に報告が行われる体制が整備されているか。内部通報システムなど損失危険管理に関する状況が業務執行ラインから独立して把握されるシステムが整備されているか ・会社に著しい損害を及ぼす事態が現に生じた場合を想定し、損害を最小限にとどめるために、代表取締役等を構成員とする対策本部の設置、緊急時の連絡網その他の情報伝達体制、顧客・マスコミ・監督当局等への対応、業務の継続に関する方針等が予め定められているか
第10条 情報保存管理体制に関する監査	・重要な契約書、議事録、法定帳票等、適正な業務執行を確保するために必要な文書その他の情報が適切に作成、保存又は管	・代表取締役等が、会社経営において情報保存管理及びその実効的体制の整備が必要不可欠であることを認識しているか ・情報の作成・保存・管理のあり方に関する規程等が制定され、かつ、当該規程を有効に実施するための社内

	理されていない結果、会社に著しい損害が生じるリスク ・重要な営業秘密、ノウハウ、機密情報や、個人情報ほか法令上保存・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 ・開示される重要な企業情報について、虚偽又は重大な欠落があるリスク	体制が整備されているか ・取締役会議事録その他法定の作成資料について、適正に内容が記録され保存される社内体制が整備されているか ・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整備されているか ・個人情報ほか法令上一定の管理が求められる情報について、役職員等に対して、当該法令で要求される管理方法の周知徹底が図られているか ・会社の重要な情報の適時開示、IRその他の開示を所管する部署が設置されているか。開示すべき情報が迅速かつ網羅的に収集され、法令等に従い適時に正確かつ十分に開示される体制が整備されているか ・情報保存管理に関して定められた規程及び職務分掌に従った管理がなされているか。情報保存管理の状況を監視するモニタリング部門が存在し、会社の情報保存管理に係る問題点が発見され、改善措置が講じられているか ・情報保存管理の実効性に重要な影響を及ぼしうる事項について、取締役会及び監査役に対して定期的に報告が行われる体制が整備されているか。内部通報システムなど情報保存管理に関する状況が業務執行ラインから独立して把握されるシステムが整備されているか

付録4.（出典：社団法人 日本監査役協会「内部統制システムに係る監査の実施基準」2007/04/05 制定）リスクマネジメント

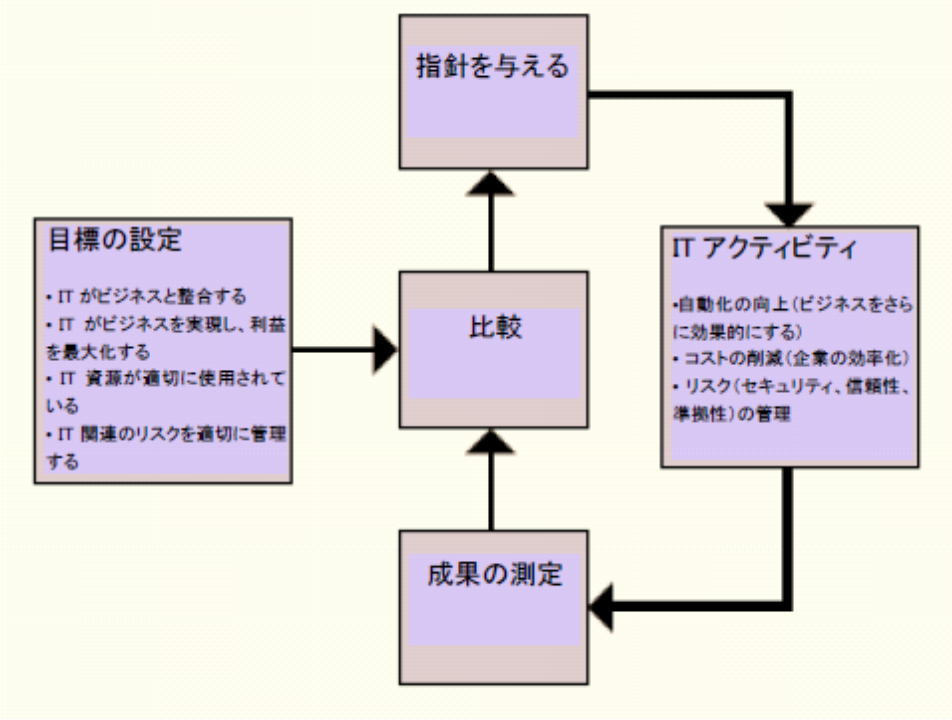
ISACA/ITGI では、IT ガバナンスとは、経営者の責務であり、企業のコーポレートガバナンスにとって不可欠な要素であり、透明性が必要な部分であり、IT ガバナンスフレームワークと整合している必要がある。経営者は情報セキュリティにより発生する事故によるサービス中断や情報漏えい機密性に対応する責任がある。また、取締役会は、情報セキュリティを企業ガバナンスの取り組みの中心的な部分として、IT ガバナンスの目標と整合し、資源を管理するために実施するプロセスと統合する必要がある。”（ISACA/ITGI、取締役のための IT ガバナンス V2 を一部修正）と定義して、下図に示すように、IT ガバナンスと共通のガバナンスを支える５つの分野として、戦略、価値創造、リスク管理、リソース管理、モニタリングを挙げている。また、これらの 5 つの要素を並列なものとして扱っている。マイケルポータも競争の戦略では、戦略面を重要視して、他の要素と区別しているように、経営者から見ると、企業の戦略や収益に直結する価値の実現を優先しがちである。



ISACA/ITGI の情報セキュリティガバナンス及び IT ガバナンスの共通の重点領域[37]

さらに、IT ガバナンス協会では、次の図に示す経営者が、IT ガバナンスを実施するためのモデルを示している。このモデルでは、経営者は、組織に対して、目標を与え、IT による具体的な行動（IT アクティビティ）に対して「指針を与え」、結果としての「成果の測定」を行い、目標との乖離を比較する。乖離が大きければ、その原因を分析し、目標に会うように指針を修正する。この際の目標の設定は、具体的に、組織が行動できるためのものでなければならない。このときの目標には、図の、「価値の実現」、「リスクの管理」とこの2つをビジネスの目標と整合するように戦略を決める「戦略的整合」が用いられる。

[37]出典：ISACA/ITGI;「取締役会のための IT ガバナンスの手引き 第２版」



IT ガバナンスの実施のための経営者の行動[38]

【 ISO 31000 のリスクマネジメント 】

ISO では、2002 年に導入された、Guide73 により、リスクマネジメントが見直された。この前提となったのは、リスクマネジメントは、各分野で、ネガティブ（望ましくない）事象をリスクが高いと考え、そのリスクを低減するというパラダイムであった。しかし、一つの分野にとって、リスクを下げるために経営資源を投入すればよいという判断は経営から見ると必ずしも、全社的な最適な解とは言えない。これは、個人情報の保護ばかりを考え、データベースに全ての経営資源を投入してリスクを下げたという事例を考えてみればよい。他の企業の分野では、投資をしないことで、収益が上げられないなどの弊害が現れる。とくに、投資家から見れば魅力が無い会社となってしまう。これでは、最適な経営判断が出来るとは言えない。そこで、リスクマネジメントを、より広く実効性のある技術として展開するためには、現実の判断を支援できるフレームが必要となり、Guide73 では、リスクの概念として、ネガティブなものだけに着目するのではなく、リスクを広くレンジのあるものとして捉えるようになってきた。すなわち、全社的なリスク対応の観点からは、ある分野ではリスクを低減するが、別のある分野では、リスクを取り、全社としてのリスクを最適化するという概念に至った。そのために、リスクの低減というのではなく、リス

[38]出典：ISACA/ITGI;「取締役会のための IT ガバナンスの手引き 第 2 版」

クの最適化という概念に拡張された。

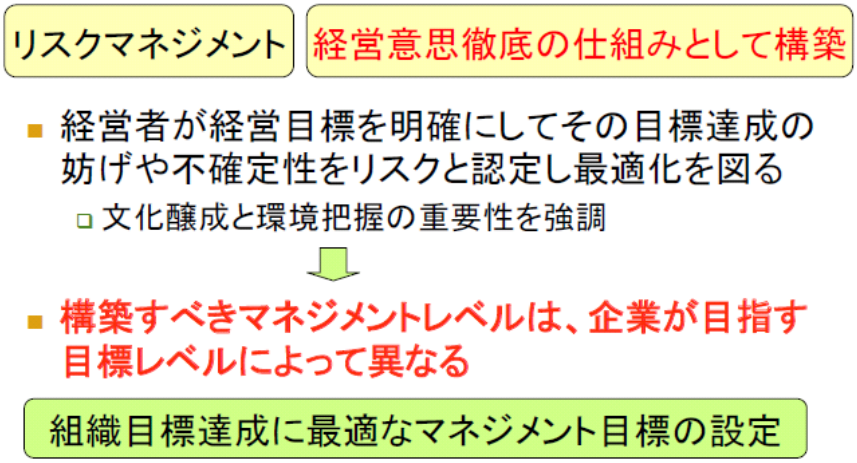
ISO 31000 では、この Guide73 でのパラダイムチェンジを引き継ぎ、組織のリスクマネジメントとしては、リスクのネガティブ、ポジティブの両面を捉えることをベースに、組織としてのリスクマネジメントのフレームワークとして提示されている。すなわち、ISO 31000 は、あらゆる組織のあらゆるリスクを対象とした規格であり、他のマネジメントガイドライン（ISO 9000 シリーズ、ISO 14000 シリーズ、ISO/IEC 27000 シリーズなど）のアンブレラ規格[39]として検討されている。したがって、今後、ISO が制定する個別のリスクマネジメント規格は、ISO 31000 と矛盾しない範囲で制定されることになっている。なお、この意味は、各マネジメントシステムのリスクマネジメント規格は、ISO 31000 を参照して、共通の構造、用語、マネジメントへの要求条件などの共通化が要請されている。ただし、規格として同一である必要はない。すなわち、各分野の特定のリスクに対するマネジメントは、各分野の個別具体的な規格により管理したほうが効率的である場合も多い。ただし、分野ごとの優先順位を経営の視点で調整する組織としての横断的なリスクマネジメントには、ISO 31000 を利用することになる。

ISO 31000 では、組織の目標達成に最適なマネジメント目標を設定することになる。すなわち、経営者が経営目標を明確にして、目標達成への阻害事象や不確定性をリスクと認定して、その全体のリスクの最適化を図ることになる。なお、この目標は、ISO 31000 が規定するのではなく、企業の経営者が決めることになる。

ここで重要な要素は、次の点である。

- 組織ミッションと経営方針の明示
- 当該組織状況と外部環境の的確な把握
- リスクマネジメント方針の策定
- リスクマネジメントの PDCA を廻すための仕組みの設計
- 実行計画の作成、リスクマネジメントの実施から仕組みの継続的改善

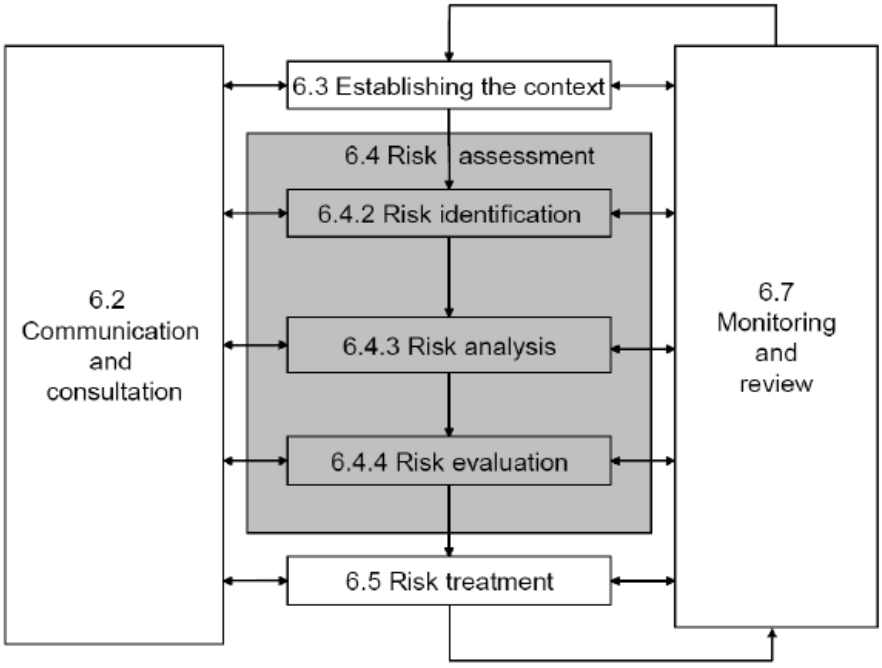
[39] 他の基準類の共通コンセプトを集約して提示するための規格。



ISO 31000 のリスクマネジメントの狙い[40]

ISO31000 は下記の構造をしている。今までのリスクマネジメントと大きく変わるものではないが、大きく違っている点がある。まず、リスクマネジメントを３つの領域に分けている。リスクマネジメントプロセス、リスクコミュニケーション、リスクマネジメントプロセスの記録、そのモニタとレビューである。さらに、ISO 31000 では、リスクマネジメントプロセスの内容をシンプルなものにしている。リスクアセスメントとそのリスクアセスメントに基づく、リスクの対策であるリスク対応の２つに分けている。今までのモデルでは、リスクコミュニケーションやリスクのモニタリングやレビューは、リスクマネジメントプロセスの結果に対するものであり、リスクマネジメントプロセスそのものではなかった。ISO 31000 では、リスクマネジメントプロセスを透明化して、すべてのプロセスについて、コミュニケーションやモニタリングができるようにしている。

[40]野口和彦；「リスクマネジメント規格 ISO31000 の概要」,2008/11/04



ISO 31000 で議論されているリスクマネジメントの構造[41]

■リスク特定

リスクの特定は、リスクを管理する対象として認知することである。組織のリスクマネジメントとしては、次のような考察が必要となる

- 組織の管理下にあるリスクも管理下にないリスクも含めることが望ましい
- 組織が設定した目標の達成を促進、妨害、低下、遅延するかもしれない事象を漏らさず一覧表にする
- リスク特定に対するアプローチ
- 概括的アプローチ：リスクが引き起こす結果とそのシナリオに基づいてリスクを見極めるために活用
- 精査的アプローチ：優先度の高い領域または問題においてリスクの特定をさらに掘り下げるために活用
- 概括的アプローチの方が、様々なリスクに対して優先順位を決められることから、精査的アプローチよりも効率が高い

■リスク解析

リスク解析の考え方は、従来、リスク特定を含むものであった。しかし、ISO 31000 では、特定を独立させて、リスクアセスメントの考え方をシンプルにした。特定されたリス

[41]図は committee draft of ISO 31000 “Risk management – Guidelines on principles and implementation of risk management”より引用。現在は最終国際規格案（FDIS）の状況。

クについて、より、細かいレベルにブレークダウンする段階である。

■リスク評価

- 意思決定では、厳密に経済的な根拠に立つと採択が認められないリスク対応処置をも容認せざる得なくするような、深刻な諸リスクについて考慮に入れることが望ましい
- 法律及び規制の要求事項、ならびに社会的責任が、財務上の費用対効果分析よりも優先する
- 組織の諸目標及び取得し得る機会の程度を考慮することが望ましい。複数の選択肢から一つを選ぶ場合、何を選ぶかは組織が置かれている状況によって異なる。
- 何が起きるかということととどのような影響があるかは異なる
- 意思決定では、リスクが置かれているさらに広い範囲の状況について考慮に入れ、そのリスクから便益を得る組織以外の他者が持つ諸リスクの許容度についての検討も含めることが望ましい。
- 周辺環境によっては、リスク評価の結果、更なる分析を実施するという意思決定が導き出されることもある

■リスク対応

リスク対応の考え方

- リスクを生み出す可能性のある活動に踏み込まないという決定を行うことによりそのリスクを回避する
- リスク回避はあってはならない形で起こることもあり、それが他のリスクの増加若しくは機会の損失に繋がることもある
- リスク回避とは、「何をしたいのか」、あるいは「したくないのか」ということの表現である
- リスク回避とはその組織の文化の一部である
- リスクの起こりやすさを変えること
- 緊急事態対応計画、不測事態対応計画、災害復旧計画などの手段により、リスクが引き起こす結果を変えること
- 他の一つまたは複数の関係者とリスクを共有すること
- ヘッジ、保険、他の類似の契約的取り決め、パートナーシップなどの相互合意に基づいた手段が望ましい。
- リスクを保有すること
- そのリスクが変化した、共有化された、または適切に受容されたなどの判断を反映した選択として保有する場合
- そのリスクの洗い出し、適切な共有化、あるいは対応ができなかったため止む無く保有する結果となる場合
- リスクを発生または持続させそうな活動を開始または継続すると決定することにより、利益を追求する

■リスクコミュニケーション

コミュニケーション活動は、あらゆるリスクに係る活動の基本となるものである。従来のリスクマネジメントモデルではリスク対応時のみコミュニケーション活動を行うとしていたが、ISO3100 では、全てのリスクのプロセスについて、コミュニケーションが必要としており、組織のリスク対策についての透明性、説明責任をより強化するものとなっている。

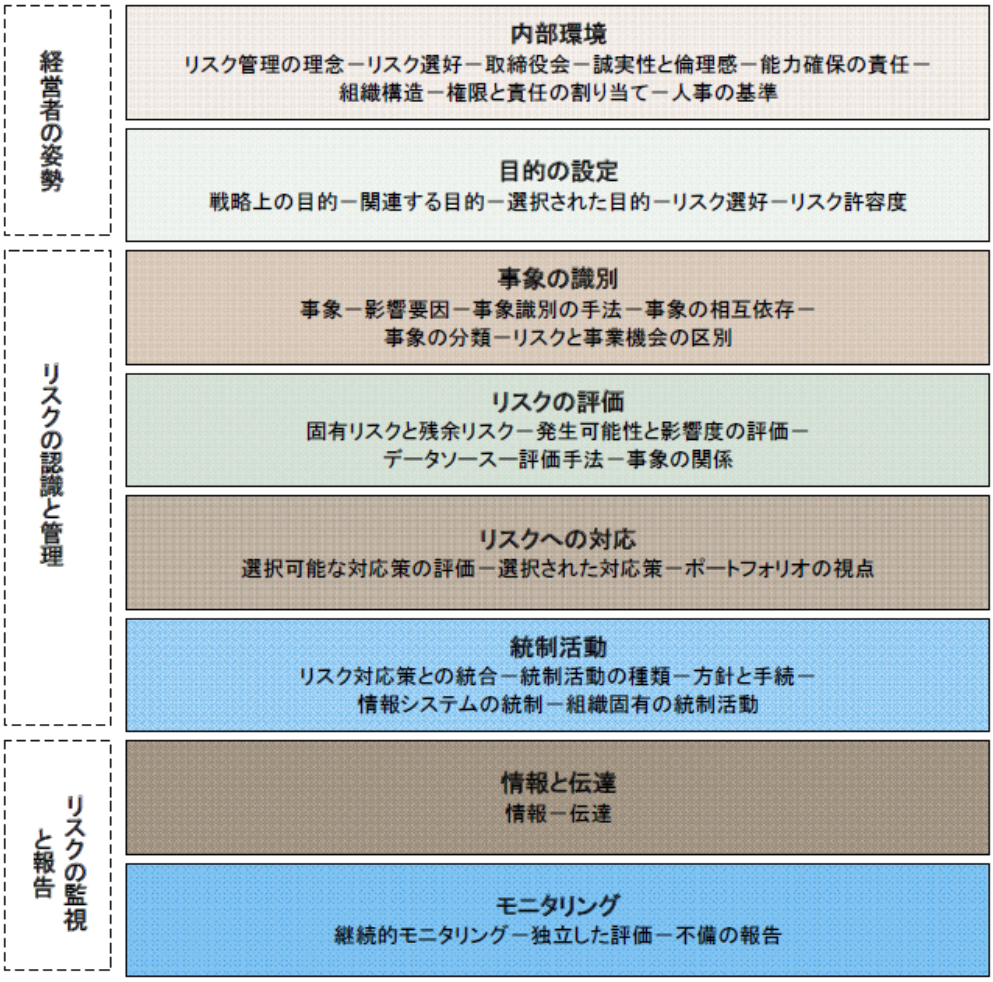
- コミュニケーション計画を策定すること
- 組織が置かれている状況の適切な把握の支援
- リスクの効果的な洗い出しの徹底の支援
- リスクを分析するための多様な領域の専門知識の収集
- リスクを評価する際のさまざまな見解に対する適切な配慮の徹底
- リスク対応時の適切な変更管理の強化
- 対応計画への承認及び支援の確保
- 利害関係者の関心の理解と考慮の確実な共有

■リスクモニタリング

従来のリスクマネジメントモデルでは、モニタリング活動は PDCA の C の段階で行うものと考えられ、リスク対応時のみしかモニタリング活動の対象とされていなかった。ISO3100 では、リスクコミュニケーションと合わせて、全てのリスクのプロセスについて、モニタリングが必要としており、リスクコミュニケーションと合わせて、組織のリスク対策についての透明性、説明責任をより強化するものとなっている。

【 COSO-ERM のフレームワーク 】

COSO-ERM は、企業の内部統制のモデルとして広く利用されている COSO モデルを拡張するなどして、企業として、全社的な観点でリスクマネジメントを実施するためのフレームワークとして提供されている。



COSO ERM フレームワーク[42]

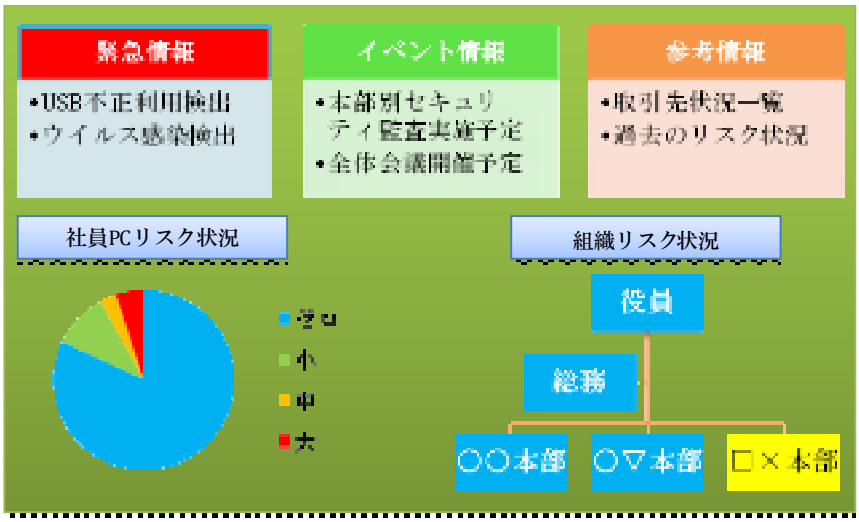
[42]出典：ISACA/ITGI;「バーゼルⅡのためのＩＴ統制目標コンプライアンスのためのガバナンスとリスクの管理の重要性」

付録5. 情報セキュリティダッシュボード

CISO は、自社の情報セキュリティ上のリスク状況を網羅的かつ直感的に把握し、必要に応じて迅速な対応を判断する必要がある。したがって、複数のモニタリング指標を評価者の視点で整理・統合できる環境を整備することが望ましい。その場合、まとまった形で情報を一覧できること、また、ある指標から読み取れる傾向の原因を探るためさらにデータ分析を詳細化できることが必要である。

例えば、自社の情報セキュリティ上の状況を一つの画面で網羅的に把握できるように配置する「情報セキュリティダッシュボード」を用いて、そうした環境を実現することができる。イメージ例を付録図 4 に示す。

情報セキュリティダッシュボードは、必要に応じてより詳細な情報を表示する機能（ドリルダウン機能）や利用者の役割・組織内の階層に応じた画面を表示できるようにして、組織内の情報セキュリティ活動とそのモニタリング指標を集中的に表示する情報セキュリティインフラストラクチャとすることもできる。階層構造は、組織の規模や事業内容の多様性に応じて２階層、または３階層で管理される。例えば IT 部門が全社 IT インフラを管理し、事業部毎に特性を持った経営を行っている会社では、IT インフラ（PC，共通サーバ）の画面と事業部毎の画面が２階層目に来るであろうし、事業部毎に IT インフラが異なる組織では、ドリルダウン機能で各事業部のマネジメントの下位階に IT インフラの管理画面を表示できるようにすることが考えられる。



情報セキュリティダッシュボードのイメージ例

例えば CISO にとっては、一つの画面で組織内の情報セキュリティの達成状況や組織が直面している情報セキュリティリスクなどを直感的に把握できることが必要である。このため、経営者向けのダッシュボードでは、詳細な現場の情報をそのまま表示するのではなく、多くの情報を適切に加工し、経営者にとって意味のある形に集約して表示することが求められる。特に、総合的に今組織がおかれている状況がどうなのかを示す信号機のよう

な「総合インジケーター」が画面上に配置されているとわかりやすい。こうすることで、このインジケーターが「青色」である限り、経営者は情報セキュリティに関して特段の意識を払う必要がないことを伝達することができる。

「情報セキュリティガバナンス研究会／ガイダンス作業部会」メンバー

（2009 年 3 月末現在，敬称略）

【主査】

大木　　栄二郎　工学院大学 情報学部 教授

【委員】（50 音順）

加賀谷　哲之　一橋大学 商学部 准教授

塩崎　　哲夫　富士通株式会社 セキュリティソリューション本部 情報セキュリティセンター長

原田　　要之助　IT Governance Institute 理事

丸山　　満彦　監査法人トーマツ エンタープライズリスクサービス部 公認会計士 パートナー

山崎　　哲　日本アイ・ビー・エム株式会社 情報セキュリティ推進室 PMO 担当

【オブザーバ】

経済産業省 商務情報政策局 情報セキュリティ政策室

【事務局】

株式会社三菱総合研究所 情報セキュリティ研究グループ