12 情セ第 373 号

情報システム部門責任者のための
情報セキュリティブックレット

2001 年 3 月

情報処理振興事業協会 セキュリティセンター

目　次

1 イントロダクション

2001 年に入り、やや減速しつつあるとはいうものの、ここ数年の米国経済の好調さには目を見張るものがあります。そして、こうした米国の成功が、IT に支えられていることは誰もが認めるところでしょう。しかし、日本と米国の IT の技術レベルにそれほど大きな格差があるのでしょうか。また、仮に技術レベルに格差があったとしても、米国 IT 関連企業の大半が日本でもビジネスを展開している現状で、本当に技術レベルの格差が経営環境を左右する主要因となり得るのでしょうか。やはりこの日米の格差は、「IT をビジネスにどう利用するか。」という経営戦略の格差によるものと考えるべきでしょう。

米国では、一般的に CIO（Chief Information Officer：情報システム部門統括責任者）は役員が務めます[1]。しかし日本では、情報システム部門の管理を担当するのは多くの場合中間管理職であり、IT 戦略策定の責任者という立場ではありません。それ故、日本の情報システム部門の責任者の権限は限定的で、IT 投資の最終権限は経理の担当役員にあったり、各事業部がそれぞれの予算で独自に情報システムを立ち上げているような状況も珍しいことではありません。このような状況下では、仮に情報システム部門が全社的な情報セキュリティコントロール[2]を実施しようとしても、CIO によって一元的に管理されている米国の事例をそのまま適用したのではうまくいきません。対策のために必要なリソースが獲得できなかったり、現場と経営の間で板ばさみになってしまったりといった問題が発生することが容易に想定されます。

一方で、情報セキュリティに関する書籍は、暗号やファイアウォールなど技術者向けの内容の書籍が大半で、管理職として必要な知識を体系立てて整理した書籍は思いのほか少ないという声も数多く聞かれます。
本書は、組織の情報セキュリティコントロールにおいて、情報システム部門の責任者が担うべき役割と、その際に必要となる考え方や知識についてまとめています。本書では、情報システム部門の責任者が、組織のセキュリティ対策上果たすべき役割は 2 つあると考えています。

①情報セキュリティコントロールに必要なリソースの確保

情報システム部門の責任者は、情報セキュリティコントロールを実施するために十分なリソースの確保を行わなければなりません。情報セキュリティコントロール実施のために必要なリソースとしては、予算の他に人材、情報、

---

1 「CIO ハンドブック」野村総合研究所（NRI）2000 年
2 情報セキュリティを確保するためのさまざまな施策。情報セキュリティ対策。

時間、他部門の協力等が考えられます。ただし、多くの日本の組織では、こうしたリソースを確保するためには、経営層の理解と協力が必要です。そこで、本書では IT ガバナンスの考え方を導入し、企業統治と情報セキュリティコントロールの関係について整理し、経営層の理解を得るための説得材料を提供します。また、情報システム部門の権限が限定的である場合には、情報セキュリティ上の役割と責任の切り分けをどうするのかといった問題がしばしば持ち上がります。そこで本書では、組織における情報システム部門の位置付けと他部門との責任の切り分けについて事例を交えながら考察を行います。また、情報セキュリティコントロールの投資効果を測定する手段として、ABC 分析とバランス・スコアカードを用いた事例を紹介します。

②実効性のある情報セキュリティコントロールの実施

情報システム部門の責任者は、組織にとって実効性のある情報セキュリティコントロールを実施しなければなりません。そのためには、正しい情報セキュリティの知識に基づき、組織で本当に必要とされている対策を、的確に選択、判断できなければなりません。そこで、本書では管理職に求められる視点として、情報リスクマネジメントの概念を紹介します。情報リスクマネジメントとは、組織の情報セキュリティコントロールを、情報セキュリティポリシーを中心とした PDS(Plan Do See)サイクルに沿って、トップダウンの視点で実施することです。また、情報セキュリティに関する国際的な動向を把握するために、情報セキュリティの国際的ガイドラインについて、その種類と利用方法を解説します。

情報システム部門の責任者は、本書を利用することで、組織の実状に即した形で情報セキュリティコントロールを立案し、現場に的確な業務指示を行うことができます。また、現場の業務担当者の報告を理解し、フィードバックするために必要な体系的な情報セキュリティの知識を獲得することができます。本書はまた、情報セキュリティに関する国際動向を把握するための資料としても利用することが可能です。

2 IT ガバナンスと情報リスクマネジメント

2.1 IT ガバナンスとは

2.1.1 コーポレートガバナンスと IT ガバナンス[3]

ここ数年、企業の大規模倒産や企業トップの不祥事が相次いだこともあり、コーポレートガバナンス（企業統治）という言葉が度々クローズアップされています。コーポレートガバナンスとは、企業活動におけるステークホルダー（利害関係者）の総合的な監視の仕組みのことを指します。例えば、「株主は自分達の預託財産を、経営者が誤った使い方をしていないか監視する。」、「経営者は、役員や事業部が、会社の資産を誤ったプロジェクトに投資していないか監視する。」といったように、企業活動に様々な監視体制を導入することによって、企業活動の正当性を保証するための仕組みが、コーポレートガバナンスです。

従来、日本ではメインバンクが企業経営者に対する監視主体としての役割を担ってきました。しかし、不良債権処理による銀行の体力低下や、国際取引の場での日本型経営スタイルの拒絶など、近年経営環境が大きく変化してきており、それに合わせてより複雑で有機的な監視の仕組みが求められるようになってきています。

コーポレートガバナンスでは、始めにベストプラクティスに基づいて企業活動が最も効率的になる目標と、それに対する具体的な企業活動を決定します。そして、この目標と目標に対する企業活動のバランスを取るために、「統制」と「資源」を導入します。（図 2-1）

ここで、「資源」とは「企業活動を推進するために必要となる人、物、金など」を指します。また、「統制」とは「目標に対する企業活動の適切性の監視」を指します。株主やメインバンク、取引関係者等のステークホルダーに対して、それぞれ統制対象を設定することにより、特定の立場に偏ることなくバランスのとれた企業運営を計るための仕組みが統制です。統制の具体的な例

[3]「週間東洋経済」（東洋経済新報社）2000 年 7 月 22 日号（情報リスクマネジメント　IT リスクの評価・モニタリング確立を）KPMG ビジネスアシュアランス　榎木千昭

としては、社外取締役の起用や執行役員制の導入などが挙げられます。

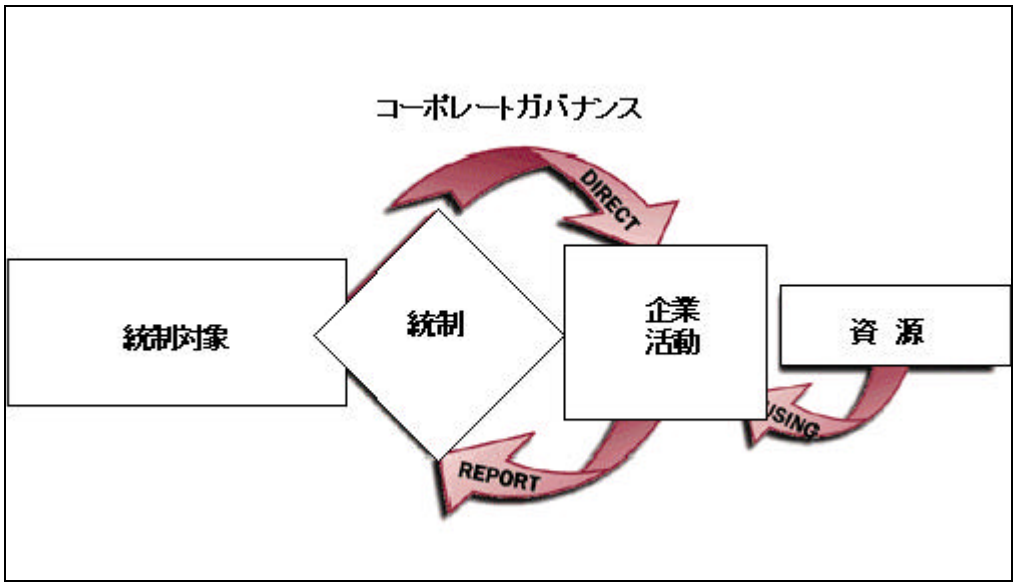

図 2-1　コーポレートガバナンスの仕組み[4]

これまでも企業活動では、意思決定のためにさまざまな情報を必要としていました。そして、あらゆる情報が IT によって取り扱われるようになった今日では、企業活動は IT の上に成り立っているとも言えます。また、IT は単に企業活動を支援するための一要素ではなく、新たな需要、ビジネスモデル、組織体系等を創造するツールとしても認められつつあります。

このように、企業活動において IT が必要不可欠となった現在では、コーポレートガバナンスの主要素として IT ガバナンスという観点が導入されるようになってきました。

IT ガバナンスとは、企業活動の効率性、信頼性等の向上のために投入された IT が、その目的に沿って有効に活用されていることを保証するための仕組みです。言い換えれば、IT を企業戦略にどう生かしていくか、あるいは IT が企業経営に悪影響を与えないためにはどうしたら良いか、という視点から統制と資源を導入し、IT プロセス[5]によって生み出されるリターンを最大化し、IT リスクを最小化するための仕組みが IT ガバナンスです。（図 2-2）

---

[4] 'COBIT Third Edition' ,IT Governance Institute, 2000.

[5] 準備活動（必要性調査や機器の選定等）、導入、利用促進、利用状況調査、廃棄といった IT に関わる一連の活動。

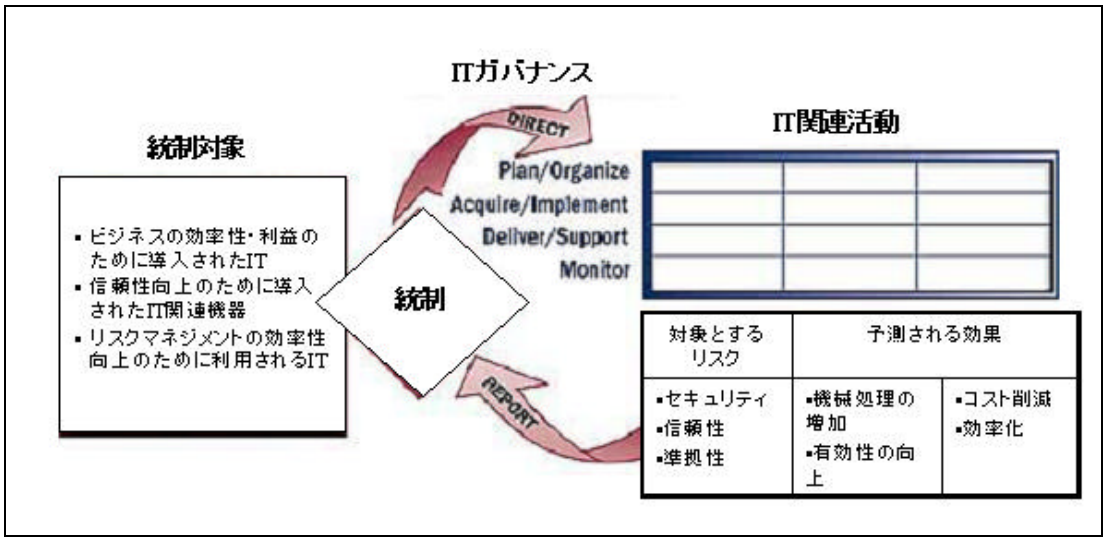

図 2-2　IT ガバナンスの仕組み[6]

2.1.2 IT ガバナンスにおける 3 つのマネジメント[7]

IT ガバナンスとは、IT プロセスによって生み出されるリターンを最大化し、IT リスク[8]**を最小化するための仕組みです。ここで IT ガバナンスには「情報リスクマネジメント」「準拠性マネジメント」「パフォーマンスマネジメント」の 3 つの側面があると考えられます。（図 2-3）**

「情報リスクマネジメント」とは、IT リスクを最小化するための取組みです。情報リスクマネジメントでは、情報セキュリティポリシーを策定し、ポリシーを中心とした PDS サイクルを運営します。情報リスクマネジメントについては第 3 章で詳しく述べます。

「準拠性マネジメント[9]**」とは、IT ガバナンスで設定される目標と活動を社会的に求められている基準と合致させるための取組みです。IT ガバナンスにおいても、コーポレートガバナンス同様、始めに IT 関連活動が最も効率的になる目標と、それに対する具体的な活動を決定します。この際、設定した目標と活動が対外的に求められる水準に適合していることを保証する仕組みが**

---

6 'COBIT Third Edition' ,IT Governance Institute, 2000.

7 **「週間東洋経済」（東洋経済新報社）2000 年 7 月 29 日号（パフォーマンスマネジメント　IT 部門の業績をどう評価するか）KPMG ビジネスアシュアランス　榎木千昭**

8 **3 章コラム 1 参照**

9 **コンプライアンスマネジメントとも呼ばれる。**

準拠性マネジメントです。特に、情報セキュリティに関する取組みは、独り善がりのものであってはなりません。自社の脆弱なセキュリティ対策が原因で、取引先や顧客、ひいては全く関係の無い第三者までリスクにさらす可能性があるからです。各企業で実施するセキュリティ対策は、それぞれの事情を反映しつつも、一方で世間一般で通用するだけのセキュリティレベルを堅持していかなければなりません。情報リスクマネジメントを実践するために意識しておかなければならない国際的なガイドラインを第 4 章で紹介します。

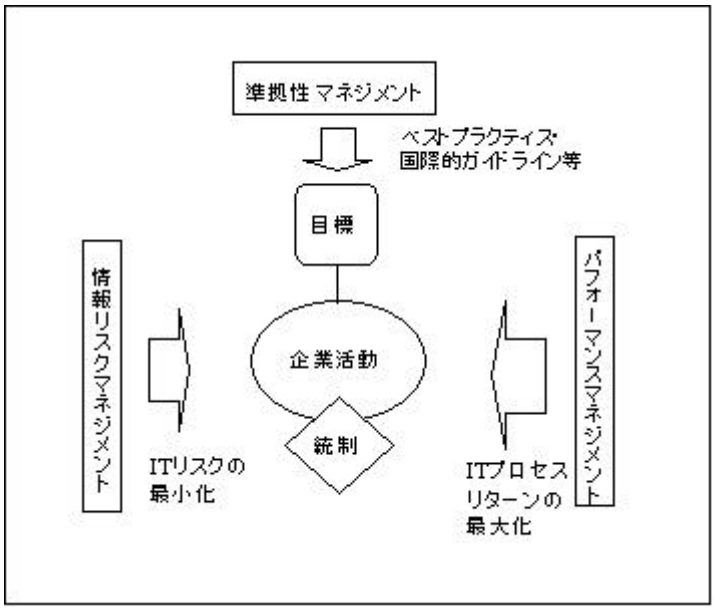

図 2-3　IT ガバナンス

「パフォーマンスマネジメント[10]」とは、IT 関連活動に投入した資源を期待通りに機能させ、IT プロセスによって得られるリターンを最大化するための取組みです。パフォーマンスマネジメントは 2.3 節で詳しく述べます。

つまり、IT ガバナンスとは、この 3 つのマネジメントの実践による相乗効果によって達成されると考えられます。

2.1.2 情報セキュリティ対策から情報リスクマネジメントへ

情報機器を利用したハイテク犯罪の増加に伴い、さまざまなセキュリティ対策が提案、実施されてきました。2000 年 1 月の省庁ホームページ連続書換

[10] 効率性マネジメント、有効性マネジメントとも呼ばれる。

え事件[11]では、ファイアウォール[12]の導入がセキュリティ確保のための必要十分条件であるかのように報道され、ファイアウォールメーカの売上が急激に増加しました。また、ノート型パソコンや PDA[13]の小型化・軽量化に伴い、紛失・盗難事故が増加し、バイオメトリクス技術[14]による認証付パソコンや別マシンでは呼び出しが不可能なハードディスクが実用化され、多くの企業が導入を検討しています。

ところで、これらの対策は企業のどの部門が担当するのでしょうか。おそらく、ファイアウォールの導入は情報システム部門が担当し、ノート型パソコンや PDA の導入はユーザ部門が担当したケースも多かったのではないでしょうか。また、プリンタやファクシミリ、スキャナといった複合機械の導入や、入出館規程の変更にあたっては総務部門が担当することが一般的ではないでしょうか。これまで日本では、各部門が必要と思われるセキュリティ対策を独自に行い、その結果として組織全体としても一定レベルのセキュリティが確保できていると判断されてきました。

しかし、自動車メーカーのリコール隠しや食品への異物混入事故の際の対応を持ち出すまでもなく、部門ごとのセキュリティ対策では、企業全体として考えるとその対策に抜け漏れが生じていても、その事実に気付かず放置され続け、結果的に事件や事故が発生した場合、全社的対応の不足が非難されることになります。情報システム部門が社内 LAN（Local Area Network）とインターネットの接続点にファイアウォールを設置し、適切な運用をしていたとしても、ユーザ部門で社員の便宜のためにダイヤルアップサーバ[15]を立て、自由に利用していたのでは、ファイアウォールがない状況と全く変わらないのです。

---

[11] 2000 年 1 月から 2 月にかけて連続して日本の省庁関連のホームページが改竄される事件が　発生した。主に、バッファオーバーフローを利用した攻撃であった。

[12] 通常セキュリティポリシーの異なるネットワーク間に設置され、あらかじめ設定されたルールに基づきネットワーク間の通信制御を行うシステム。（不適切な設定ではセキュリティ対策にならない。）

[13] Personal Digital Assistance の略で、住所録，スケジュールなどの個人情報管理やデータ通信に用いる小型の情報機器。

[14] 指紋認証や、虹彩認証、声紋認証などの身体的特徴をデジタルに変換して，ファイリングされた属性と ID を関連付け個人を特定する。機密性の高い建物の入退室管理に使われているケースが多い。

[15] 遠隔地から電話回線などを利用して LAN に接続できるリモートアクセスサービスを提供するサーバ。

インターネットを利用した国際ハイテク犯罪の増加などに伴い、日本のモラルの範囲内で有効であると考えられてきた、部門ごとにセキュリティ対策を実施するボトムアップ方式では明らかに限界が露呈しつつあるのです。

今日のビジネス環境においては、全社横断的なセキュリティ対策が必要です。この時に求められる考え方が、IT ガバナンスの一側面でもある情報リスクマネジメントです。情報リスクマネジメントでは、トップダウン方式で全社的な視点からセキュリティ対策を実施します。そして、情報リスクマネジメントの確立に必要不可欠な要素が情報セキュリティポリシーです。情報セキュリティポリシーとは、組織の情報セキュリティに関する統一方針を示した文書であり、情報セキュリティを維持するための様々な取組みについて包括的に規程された文書です。情報リスクマネジメントの過程で実施される様々なコントロールは、全てこの情報セキュリティポリシーに基づいたものでなければなりません。

情報セキュリティポリシーを策定せず、その都度セキュリティ対策を講じていく場当たり的な方法では、自ずとその対策内容にもムラが生じてしまい、結果として全社均質なセキュリティレベルを維持することができません。セキュリティとは、最も対策が遅れている 1 箇所を狙われてしまうと、他の箇所で実施されていた対策が全て無効になってしまう性質のものです。このようなほころびを作らないためにも、情報リスクマネジメントを確立し、情報セキュリティポリシーに基づくトップダウン型のセキュリティ対策を実施することが重要なのです。

事例 1　システム開発における IT ガバナンス

ある中堅建設会社は、現場主導で進む情報化を情報システム部門がまとめあげることができず、全体の管理に手を焼いていました。

阪神大震災の復興応援のために、現場経験のある社員を神戸に送ったところ、現場所属のシステムのわかる人間が社内にいなくなり、トラブル対応のために情報システム部門に SOS が寄せられました。しかし、情報システム部門では、各部の実態の把握すらできておらず、なすすべがありませんでした。

現場主導の情報化は、ニーズを的確に理解していると思われがちですが、専業ではないため、いざという時に本業が優先されトラブルへの対応が遅れたり、該当社員の退職、異動等によって後任が不在になるなどの問題点も数多くあります。また、現場主導の情報化は部分最適に陥りがちです。

このような危険性を回避するためには、IT ガバナンスの視点を、情報システム部門のみならず現場の情報システムユーザーも理解しておく必要があります。

2.2 セキュリティ対策における情報のオーナーシップ

IT ガバナンスの視点から、情報リスクマネジメントを実践する重要性が理解できたとしても、実際の対策を取ろうとした段階で「担当部署が決められない」という、大きな壁にぶつかることが珍しくありません。

こうした問題が発生する原因には 2 つの事柄が考えられます。1 つ目の原因は、日本では一般的に情報が誰に所属しているのかという、情報のオーナーシップが不明確ということです。情報システム自体は、その所属と担当者が明確化されていても、システムに登録・保存されているデータの責任者までを意識して管理体制を整えている企業は少ないのではないでしょうか。情報システム部門の責任者は、まず情報システムとデータの所有者が異なる場合があるという現状を理解する必要があります。その上で情報システムと情報をどのように管理すべきなのかを考えなくてはなりません。情報システムの管理責任がどこにあるのか、情報の所有者が誰であるのか、この両者が異なる場合はどのような情報伝達経路を整備する必要があるのかを考慮する必要があります。事例 2 では、営業部門が E-Commerce[16]用サーバの構築を行う場合を例にこの問題について考察します。

2 つ目の原因は、セキュリティ対策を実施するためには複数の部門や組織が参加しなければならない場合が多いということです。自社内においても、部門間で折衝を行い主管部署や作業分担を決めていくことは大変な労力を要します。これに外部の組織が関連してくる場合は、更に問題は複雑です。事例 3 と事例 4 では、アウトソーシングを例にこの問題について考察します。

言うまでもなく、組織内に蓄積された情報は重要な資産です。この資産を組織の壁にとらわれずにいかに有効に、かつ安全に利用するかを考えることは IT ガバナンスにおいて欠かすことのできない視点です[17]。

---

16 オンラインショッピングやオンライン取引サービス用の Web サーバ。クレジットカードなどの機密情報をやり取りする必要があるため、通常送受信するデータを暗号化し、データの内容を第三者に知られないようにする機能が用意されている。

17 「バリューベース・ナレッジマネジメント」ダニエル アンドリエッセン（ピアソン・エデュケーション）2000 年

事例２　部門を越えた情報リスクマネジメントの必要性

セキュリティ対策の実施時には、情報の重要度と同時にその情報に誰がどのような権限でアクセスすることが可能なのかを考慮する必要があります。例えば、営業部門で購入した E-Commerce 用のサーバを物理的安全性の確保のために、壁や天井を強化し、災害対策を施したサーバ管理区域の一角に設置したとします。この区域の管理部門は情報システム部門で、バックアップテープの交換などのために入室が許可されるのは情報システム部門の社員だけです。このような場合、例え営業部門の社員であっても、勝手にバックアップテープを持ち出すことはできません。では、情報システム部門の社員であれば、このバックアップテープからデータを呼び出す権限があるのでしょうか。このような場合には、情報システム部門の社員がテープ交換やバックアップログ確認のために物理的にサーバにアクセスすることは許可するが、勝手にテープを該当区画以外に持ち出したり、テープの内容を読み出したりすることができない仕組みが必要になります。

では、データの所属先だけでシステム管理をまかなおう、という考えから営業部門が情報システム部門に断り無く、自部門で E-Commerce サーバを立てたとします。この場合、情報と情報機器の所属先は明確です。一体、何が問題なのでしょうか。近年、設定の容易なサーバソフトが提供され、IT 専門家でなくとも簡単に E-Commerce 用の仕組みが作れるようになりました。そのため、営業部門などの現場が直接顧客やサプライヤーと取引をするためのシステムを作り、公開していることが珍しくありません。しかし、システムの運用管理は構築以上に難しく、特に外部ネットワークと接続している場合、セキュリティ対策には非常に多くの時間と費用を要します。現場でこのようなセキュリティ対策まで行うことは困難な場合が多いのではないでしょうか。例え社内ネットワークと接続されていないにしても、社名を冠したサーバが攻撃される、あるいは頻繁にダウンするといったことは組織全体のイメージダウンにつながります。

このような状況を避けるためにも、情報のオーナーシップを明確にするとともに、情報リスクマネジメントの考え方を現場にも浸透させることが必要なのです。

事例３　アウトソーシング[18]

社内でシステムの運用ノウハウがない場合や、リソースが不足している、コアコンピタンス以外の業務にリソースを割きたくない、といった理由から ASP（Application Service Provider：アプリケーションサービスプロバイダ）を選択するケースが増えてきています。この場合、システム自体の所有権は受託者であるアウトソーサー[19]にあります。では、データの所有者は誰なのでしょうか。データの所有者はアウトソーシー[20]である委託者になるであろう、ということは感覚的には理解できるでしょう。しかし、アウトソーシングの契約にあたって、そのような文言が契約書に明記されているでしょうか。システムの稼働率やサーバの設置環境に対する条項が覚書に記載されていても、データに対するアウトソーサー側のアクセス権限を定めていない限り、無断でサーバ内のデータを参照されても、契約違反ではありません。

また、アウトソーシングにあたっては、アウトソーサー側のセキュリティレベルが、自社のセキュリティレベルを満たしているかどうか確認しなければなりません。しかし、セキュリティレベルの確保を求める条項が、契約書に明記されているでしょうか。データ入力業務の委託にあたってはタイプミス率が何%以下であること、といった条項が覚書に記載されることがあります。しかし、データのセキュリティ確保のための項目がこれだけだと、タイピング作業を行うモニタが窓に向かっており、向かいのビルから撮影可能だったとしても、契約違反ではありません。

アウトソーシングは、自社のリソースを有効活用し競争力を高めるためにも有効な手段です。しかし、安易な外部委託は情報漏洩、効率性低下、将来の技術力の低下といった危険性をもたらす可能性があることを理解した上で適切な契約を結ぶ必要があります。

また、IT がコアビジネスではないとの理由からシステム管理部門全てを社外に頼る企業もあります。しかし、いまや IT はビジネスを支える根幹であり、ビジネスをいかにして IT に乗せるかを考え、どのようにして資産を守るかというセキュリティ対策をとりまとめるためには、社内状況を的確に把握することが可能な人材が求められます。自社の情報価値の創造やセキュリティ確保のためには、適宜業務の切り出しを行いながらも、システム部門管理責任者や情報セキュリティ責任者は社内に設置する必要があります。

18「IT アウトソーシング戦略」キャシー・M. リピン（ＮＴＴ出版）2000 年
「戦略的アウトソーシングの進化」西口敏宏（東京大学出版会）2000 年

19 アウトソーシングを依頼される側で、受託者とも呼ばれる。

20 アウトソーシングを依頼する側で、委託者とも呼ばれる。

事例 4　アウトソーシングと SLA[21]

J.P Morgan の CIO は、今後益々激化する市場を常に追い続ける為の戦略の 1 つとしてアウトソーシングを検討していましたが、アウトソーシング会社には、それぞれ得手不得手があり、1 社に集中して依頼するのはリスクが高いと認識していたため、アウトソーシングに踏み切れずにいました。

そこで彼は、TPI 社（コンサルティング会社）に相談したところ JV（ジョイントベンチャー）形式の提案を受けました。彼は、その提案を受諾し TPI 社にベンダー選定のコンサルを依頼しました。検討期間 12 ヶ月。そこで決定したのが CSC、アンダーセンコンサルティング、AT&T ソリューションズ、ベルアトランティックの 4 社共同であり、7 年契約、$2Billion の契約が成立しました。契約書の厚さは 1m強にもなりました。それぞれの役割は、以下の通りです。

- CSC：稼動後の全体コーディネート、データセンターの運用
- アンダーセンコンサルティング：業務アプリケーションの開発
- AT&T ソリューションズ：グローバルネットワークの管理
- ベルアトランティック：デスクトップサービス

上記 4 社と J.P Morgan で「ピナクル・アライアンス」というヴァーチャルな企業体を結成し、システムの受託を行う形態を採用しました。また、TPI は、稼動までの上記ベンダーの選定、人事処遇・教育のコンサルテーション、J.P Morgan の資産をアウトソース先へ売却するにあたってのコンサルテーションを行いました。

これらの会社は、このプロジェクトを成功させるのは相互の信頼関係であることを十分に認識しており、基本的に出身会社を意識することなく業務に従事しています。例えば、ピナクル・アライアンスのメンバーの名刺には、出身会社は明記されておらず「ピナクル・アライアンス」だけが記述されています。また、J.P Morgan からそれぞれのアウトソース先への報酬は、個々のサービスレベルに対して支払われるため、J.P Morgan 内に設置してある品質管理チームとピナクル・アライアンスのメンバー間では常に密なコミュニケーションが図られています。このように、複数の企業がそれぞれの役割を明確に認識した上で行われるアウトソーシングでは、企業のコアコンピタンスを明確化し、それぞれの強みを生かすことができます。

そのためには、非常に複雑で詳細に明文化されたサービスレベル契約が必要なのです。

---

[21] 「Foundations of Service Level Management」Rick Sturm（SAMS）2000 年

しかし、J.P Morgan 社のように法務の専門家を数多くかかえる企業でさえ、サービスレベル契約のためにコンサルティング会社を雇いました。このサービスに対する契約をSLA（サービスレベルアグリーメント）といいます。

SLA とは、サービスレベル同意書とも呼ばれる、アウトソーサーと依頼者の間において取り決めたサービスレベルにおける合意事項や合意契約のことを指します。

サービスレベルとは、アウトソーサーより提供されるサービスの品質とコストの関係を指します。例えば、システム開発のアウトソーシングを依頼した場合は、システム受託者から提供されるシステムのクオリティとコストの関係をさします。システム自体のパフォーマンス（稼働率・レスポンスタイム・エラー発生率等）のみではなく、人的対応におけるパフォーマンス（問い合わせに対しての回答時間・障害発生時の対応時間等）まで含むこともあります。

この同意書を利用することで、サービスレベルを明確にすることが可能になり、アウトソーシングリスクを低減し、サービスの品質を向上させることが可能になります。

SLA 策定にあたっては、プロジェクト開始前に参加メンバーの SLA に対する理解を高め、開始後にはサービス要素に関する詳細な情報収集・サービス定義・パフォーマンスデータ収集などを経て、パイロット SLA を作成、レビューを繰り返して SLA を策定するというプロセスを経ます。

欧米ではアウトソーシングにあたっては SLA の締結を義務化する企業もあるなど SLA は活発に利用されています。しかし、日本では総論賛成各論反対の状況です。これは SLA がなくともビジネスに支障はないのではないか、という考えが依然として存在すると同時に、SLA を有効性に機能させるためのリソースが不足していることも原因です。

ビジネスのグローバル化に伴い、日本国内でも SLA の重要性は今後ますます増大すると思われます。自社内でリソースを確保できない場合は、SLA サービスの提供も始まりつつあります。IT 投資効率の向上、システムの品質・コスト向上のためにも、SLA の締結は重要です。今後日本においてもアウトソーシングの成功のために、SLA サービスが盛んになると考えられます。

2.3 セキュリティ対策予算の確保

2.3.1 効率性評価手法を利用したパフォーマンスマネジメント

IT ガバナンスと情報リスクマネジメントの考え方は、セキュリティ対策費用を獲得し、組織内の協力を得るための経営層に対する説得材料と成り得ます。

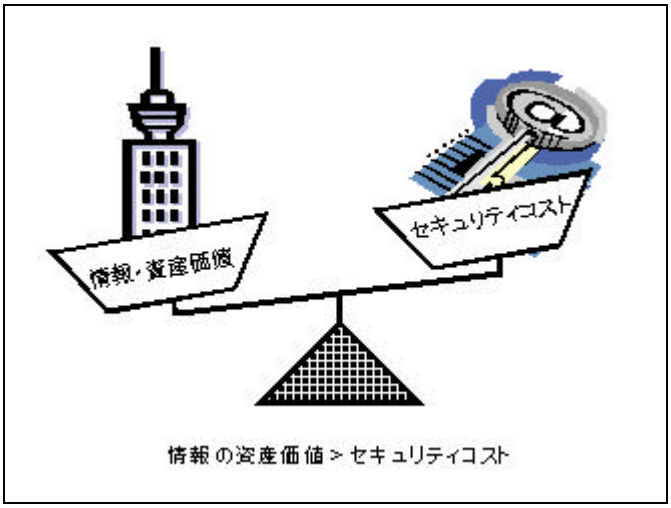

図 2-4　情報セキュリティコストと情報資産価値の関係

しかし、全社的に売上が伸び悩む中では、間接部門の経費を削減する要求が強くなりがちです。このような状況においては、セキュリティ対策費用が守るべき情報資産価値に見合っているのかを分析し、対策費用が無駄ではなかったことを具体的に示す必要があります。また、情報システム部門の業績評価や IT 投資結果の効率性評価を求められることもあります。これらの場面においては、IT 投資効率を数値化することが有効です。

本節では、企業のパフォーマンスマネジメントを評価する上で有効な ABC 分析とバランス・スコアカードを紹介します。[22]

---

[22] 「ABC マネジメント理論と導入法」アーサーアンダーセン（ダイヤモンド社）1997 年
「ABM で業務が変わるコストが下がる」PWC コンサルタント（PHP 研究所）2000 年

例 1　ABC 分析[23]

ABC 分析（Activity Based Costing：活動基準原価計算）とは、受注処理や日程計画等、間接業務の一つ一つに値札を付け、製品毎に実際にかかった作業を割り出し、正確な間接費をつかむ分析手法です。従来の原価計算方法では、間接費の配賦によって原価が歪められるため、よく売れているが赤字になっている製品に気が付かないといった問題がありました。しかし、ABC 分析では、間接費をアクティビティ（課業のまとまり）毎に算定してそれぞれの消費度合いに基づいて該当する製品にひもづけるため、従来原価計算と違い正しい原価の把握が可能となります。そのため、業務改善の指標とすることができ、正しい予算の作成や間接コストの低減といった効果を期待することができます。

例えば、従来はセキュリティ対策費用というと、セキュリティ対策機器予算など実際のセキュリティ対策コストの一部だけを取り出して扱うことが多く、トータルコストを算出することが難しいとされてきました。これは、人件費が販売管理費や一般管理費の中に吸収されてしまい、セキュリティ対策によってどの部門でどれくらいの人件費が発生しているのか、あるいはセキュリティ問題が発生した場合には、どの部門でどの程度の人件費が発生するところをセキュリティ対策によってどのくらい低減しているのか、といった側面を扱うことができないためです。

そこで、ABC 分析を用いて、システム管理部門・総務・その他部門といった各部門においてセキュリティ対策に使われた業務時間を収集、集計することで、機器購入費などの直接費のみではなく、間接費を含めたコスト算出を行う方法が考えられます。（図 2-5、図 2-6）

[23] 「ＡＢＣの基礎とケーススタディ～ＡＢＣからバランスト・スコアカードへの展開～」桜井通晴（東洋経済新報社）2000 年

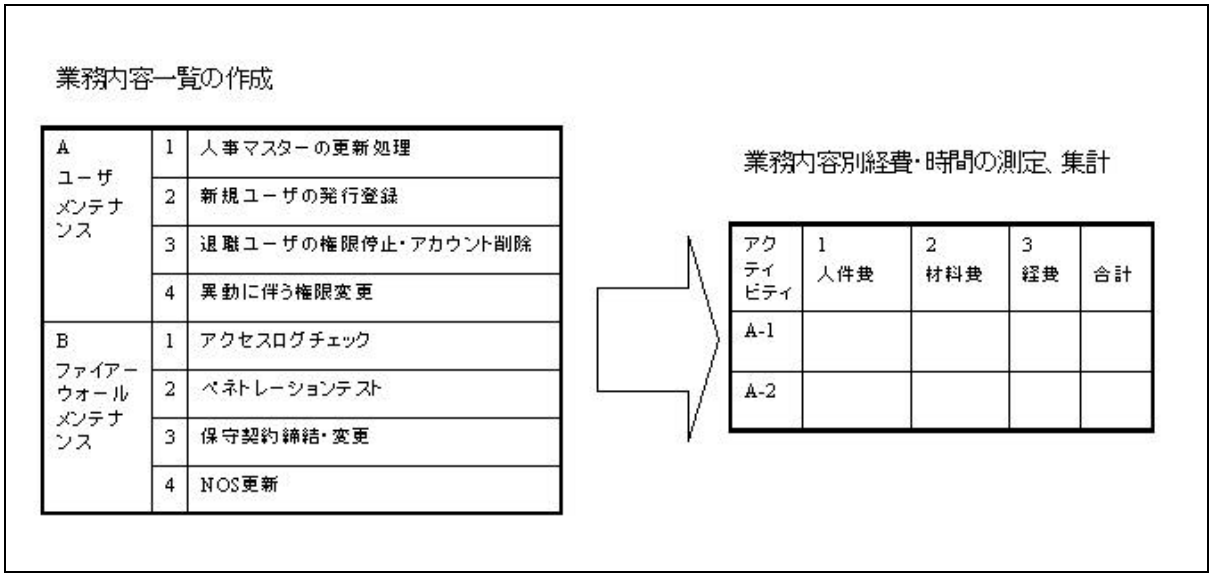

図 2-5　セキュリティ対策業務分析例

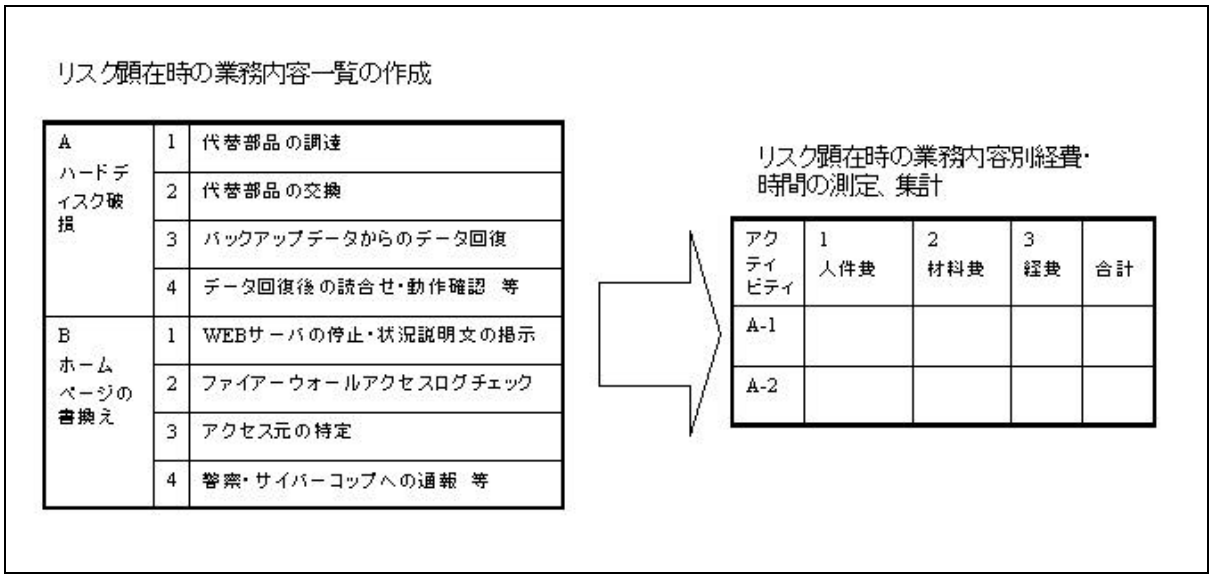

図 2-6　リスク顕在時の業務分析例

また、ABC 分析の結果を用いて、セキュリティ対策の各活動と、セキュリティ問題が発生した場合の活動を比較することで、セキュリティ対策の効率性を数値化することも可能です。

しかし、ABC 分析では各活動を当月期内で結びつけるため、教育、啓発に関する投資のような投資と効果に時間的隔たりが大きい間接費の効果測定には限界があります。また、活動と直接因果関係の認められる影響のみを扱うため、広範囲に渡って影響する投資においては、分析に限界があります。しかし、単純な分析方法であるため、時系列的な評価に難があるとはいえ、自

社内で容易に実施することが可能であり、IT 投資やセキュリティ対策にとどまらず、間接費用の短期的効果を測定するためには有効な手段だといえるでしょう。

例 2　バランス・スコアカード[24]

投資と投資効果の間に時間的隔たりの大きい業務の業績評価にあたっては、バランス・スコアカードを利用することが可能です。バランス・スコアカードとは、企業ビジョンや戦略を一貫性のある KPI（Key Performance Indicator:業績評価指標）で評価する業績評価手法でノーラン・ノートン社が業績評価手法の実態調査用に開発した業績評価モデルを起源としています。もともとは経営全般にかかわる業績評価手法ですが、情報システム部門に対してのみ適用することも可能であり、これを「IT バランス・スコアカード」と呼びます。

IT バランス・スコアカードでは、以下の 4 つの視点に該当する KPI を選択して IT 部門の業績評価を行います。KPI は各視点毎に 1 つ以上選択されます。また、企業の実情にあわせこの視点を変更・増減することで、企業戦略等の実態に則した業務評価をすることが可能です。[25]

① ユーザ志向：ユーザは IT 部門をどのように評価しているか。
② オペレーションの優秀さ：IT プロセスはいかに効率的かつ効果的か。
③ ビジネスへの貢献：経営層は IT 部門をどのようにして評価しているか。
④ 将来志向：IT は将来のニーズにいかによく適合しているか。

情報セキュリティコントロールは、将来志向の視点から大きな KPI となり、企業の長期的成長のために果たす役割を数値化して表現することが可能になります。また KPI の評価結果は、図 2-7 のように認知しやすい形に加工して利用されます。

---

[24] 「バランス・スコアカード経営」松原恭司郎（日刊工業新聞社）2000 年
「バランススコアカード」ロバート S キャプラン（生産性出版）1997 年
「コーポレイトブランド経営」伊藤邦雄（日本経済新聞社）2000 年
「バランスト・スコアカード～理論と導入～」伊藤嘉博（ダイヤモンド社）2001 年

[25] 「The Strategy Focused Organization」ロバート S キャプラン（HBS）2000 年

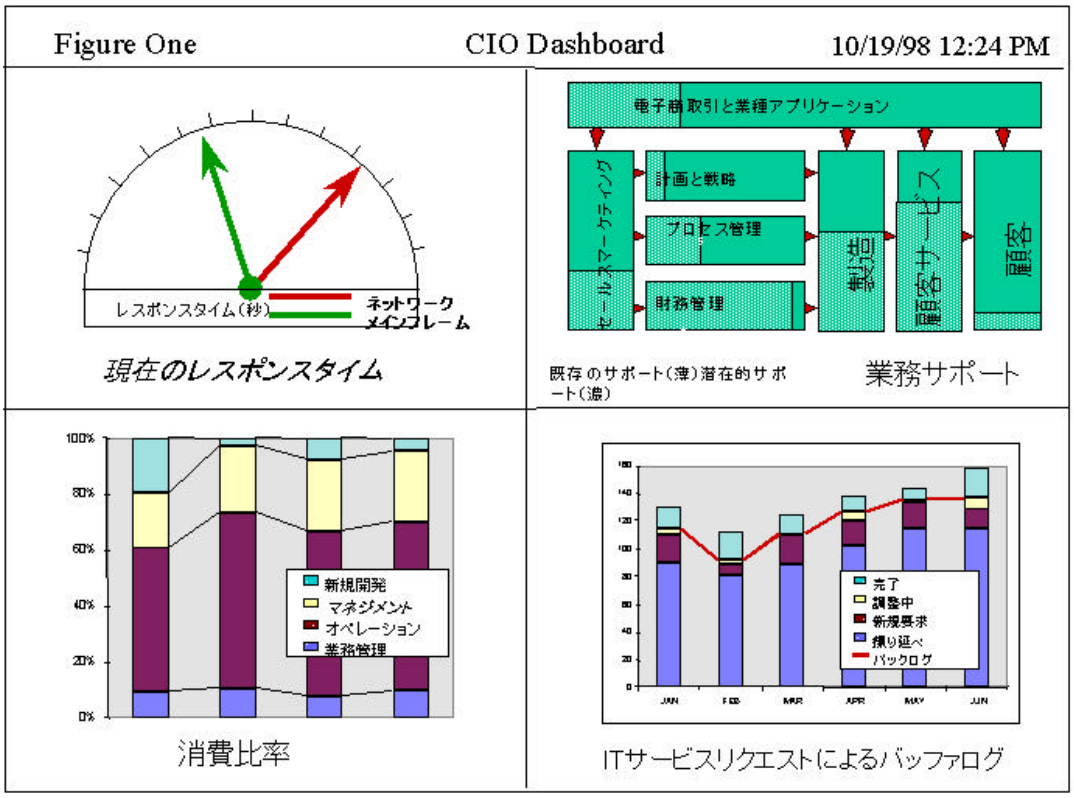

図 2-7　CIO ダッシュボード

図 2-7 はバランス・スコアカードによる評価結果を加工した CIO ダッシュボードと呼ばれる図の例です。左上図の「現在のレスポンスタイム」は、ネットワークとメインフレームマシンそれぞれの要求から応答までの応答時間を表示しており、ユーザのシステムに対する利用満足度と IT 部門のオペレーションの優秀さを測ることができます。

右上図の「業務サポート」は複数の棒グラフから構成されています。製造や顧客サービス等の業務プロセスで利用されている IT に対する要求に対して、現状では何パーセントのサービスが提供できているかを図示しています。左下図の「消費比率」は、組織内の情報機器リソースがそれぞれ何パーセント利用されているのか、という利用効率を表示します。これを定常的に監視することによって、増設すべき機器や無駄な投資箇所を把握することが可能になります。

右下図の「IT サービスリクエストによるバッファログ」は、IT サービスに対する現場からの要望や業務依頼がどの程度当月内に処理されたか、翌月に繰り越されたか、あるいは却下されたかを示しています。これは、IT 部門の業務処理効率を測定できると同時に、却下されたリクエストが大量に発生し

ている場合には、業務手順が大幅に変更された等の理由により IT の利用目的や利用方法が実状に合わなくなった可能性があると判断することも可能です。情報システム部門の責任者はこの結果をもとに、現場との業務調整や業務手順の変更を検討することができます。

バランス・スコアカードは、システム管理業務やセキュリティ管理業務を逐次参照することなく、全体効率を一目で確認することができるため、多くの業務を抱えている情報システム部門の責任者にとって有効なツールと成り得ます。また、情報システム部門の業績を数値化することが可能なため、経営陣がリアルタイムで業績評価や業績認識を行うためのツールとして利用することも可能です。

情報システム部門の責任者や経営者は、バランス・スコアカードを利用した効率性、可用性動向のグラフを利用することで、個々の業務状況を逐次参照することなく、自社のパフォーマンスマネジメントの状況を感覚的に把握することができるようになります。

ABC 分析と比較すると、自社戦略のブレイクダウンや KPI の選定など難しい面も多いと思われますが、間接費・直接費の現在と将来における影響を測定・可視化することが可能な手法です。

米国では、2001 年 1 月現在で、フォーチュン 500 企業の約 4 割がバランス・スコアカードを採用しており、日本でもバランス・スコアカードを利用した情報システム部門評価コンサルティングサービスや、CIO ダッシュボードのようにバランス・スコアカードの評価結果を可視化するシステムが提供され始めています。

2.3.2 情報リスクマネジメントの予算獲得における特殊性

情報システム部門が担当している日常業務は、セキュリティ対策を含む情報システムの運用管理業務と、ユーザ教育やヘルプデスクなどのユーザサポートが中心ではないでしょうか。これらの業務は、企業の情報セキュリティを堅持していくためには必要不可欠な業務ですが、実施即効果が現れる性質のものではないため、他部門や経営陣から見るとその効果が見えにくいと言わざるを得ません。そもそも、セキュリティ対策はリスクを低減し顕在化させないことが目的のため、投資効果が可視化されることはあまり考えられません。情報リスクマネジメントには「投資を行えば行うほど効果が実感できなくなる」という特殊性があるのです。そして、この特殊性のために、情報リスクマネジメントを導入し、様々なセキュリティ対策を講じたものの、時間の経過と共に自社の対策に安心しきってしまい、IT 技術やビジネス環境の

変化に伴うリスクの変化に気付かず、結果としてリスクが発現してしまう恐れがあります。

また、企業が抱える全てのリスクに対応するためには、膨大なコスト（時間・費用・人材等）が必要となります。そのため、情報リスクマネジメントでは、発生する可能性が低いリスクに対しては、対策は行わないあるいは後回しにするリスク受容という方針を取ります。ここで、万が一対策が行われていない（後回しになっていた）リスクが発現した場合、そのことを理由に情報リスクマネジメントへの投資が全て無駄であったと判断されてしまう可能性もあります。

このような感覚的な判断を避けるためにも、ABC 分析やバランス・スコアカードを利用した効果測定は有効です。

3 情報リスクマネジメントの実践[26]

3.1 情報リスクマネジメントサイクル

情報リスクマネジメントとは、IT ガバナンスの一側面を捉えた考え方であり、具体的には、情報セキュリティポリシーを中心とした PDS サイクルに沿ってトップダウンの視点で組織のセキュリティ対策を実施することです。

ビジネスとビジネスを取り巻く環境は刻々と変化していきます。そして、ビジネスの変化に合わせて、情報システムも絶えず変化していきます。情報システムを取り巻く状況が変化することによって、それまでは想定されなかった新たなリスクが発生することもあります。また、リスク自体の大きさが変化することも考えられます。一度導入した情報セキュリティコントロールが、永久的に有効である保障はどこにもありません。そのため、セキュリティ対策導入後も継続的に PDS サイクルを運用し、変化し続けるリスクを常に捕捉していなければなりません。この継続的な取組みのことを特に情報リスクマネジメントサイクルと呼びます。

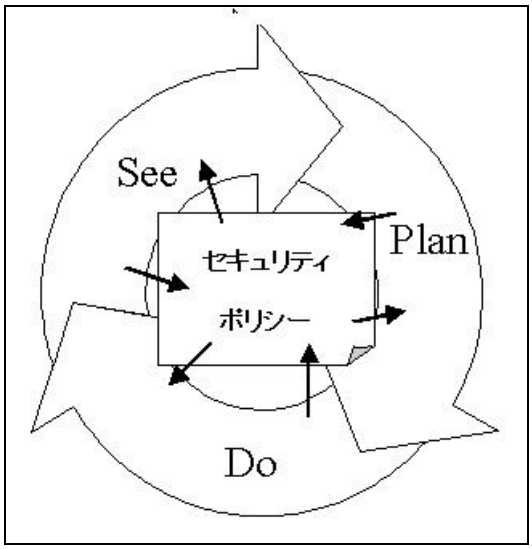

図 3-1　セキュリティポリシーと情報リスクマネジメントサイクル

---

[26] **「ネットビジネスのセキュリティ」島田祐次・榎木千昭・満塩尚史（日科技連）2000 年**
「セキュリティポリシーでネットビジネスに勝つ」三輪信雄（NTT 出版）2000 年
「ネットワーク危機管理入門」上原孝之（SE）2000 年

図 3-1 では、情報リスクマネジメントサイクルは、情報セキュリティポリシーに基づき、Plan、Do、See の各フェーズを繰り返し行うことによって達成されることを表しています。

また、Plan、Do、See の各フェーズ間の関係は図 3-2 のようにも表すことができます。図 3-2 は、セキュリティポリシーに基づき Plan フェーズで目標とその目標を実現するためのプランを立案し、Do フェーズでは立案されたプランに沿ってセキュリティ対策を実施し、結果として生じた目標と現実のギャップを See フェーズで検証することを表しています。

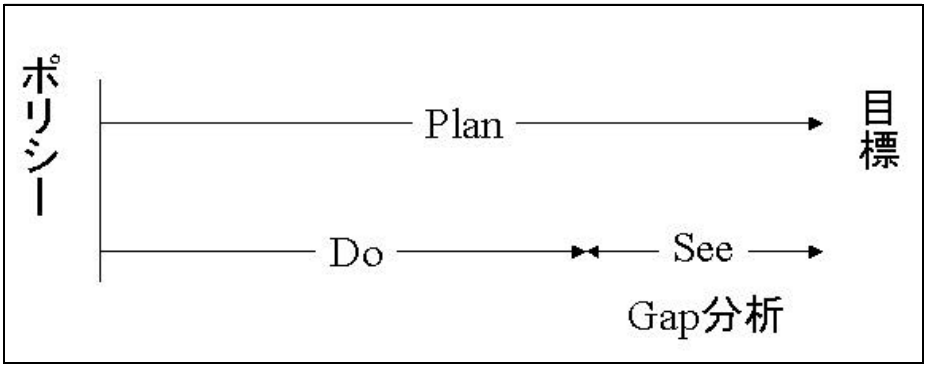

図 3-2　3 フェーズ間（Plan、Do、See）の関係

実際には、Plan、Do、See の各フェーズ毎に実施しなければならない作業は想像以上にボリュームがあり、情報システム部門だけではなく全社の協力の下ではじめて実現可能なものです。また、必要とされるリソース（予算、人材、情報、時間等）も、情報システム部門に限らず、全社横断的に必要とされることが数多くあります。

次節からは、具体的に各フェーズで実施される様々な活動について紹介していきます。

3.2 情報セキュリティポリシーの策定

情報リスクマネジメントを通して実践される情報セキュリティコントロールは、全て情報セキュリティポリシーに基づく内容でなくてはなりません。情報リスクマネジメントでは全ての活動に先立って、組織全体の情報セキュリティポリシーを策定します。

3.2.1 情報セキュリティポリシーの対象範囲

情報セキュリティポリシーとは、組織の情報セキュリティに関する方針を示した文書であり、情報セキュリティを確保するための様々な取組みについて包括的に規定された文書のことを指します。実際には、情報セキュリティポリシーといっても、各ガイドライン毎にその対象範囲の解釈に若干の違いが見受けられます。

例えば、BS 7799[27]では情報セキュリティポリシーの保護対象である情報は「情報は多くの形で存在し得る。情報は紙に印刷され、又は紙に書かれ、電子的に保存され、郵便又は電子的手段によって伝達され、フィルム上に示され、もしくは会話においても話される。情報は、どのような形のものであろうとも、また、どのような手段によって共有又は保存されようとも、常に適切に保護されることが望ましい。」とされています。

また、「金融機関におけるセキュリティポリシー策定のための手引書[28]」（金融情報システムセンター）では、情報セキュリティポリシーの保護対象である情報資産を以下のように定義しています。

情報資産とは、以下の「情報」及び「情報システム」を指しています。

情報：コンピュータシステムや磁気媒体等に保存されているデータのみならず、紙に印刷されたものやコンピュータシステムに入力される前のメモ及び社員の会話や個人の記憶をも含んでいる。

情報システム：ハードウェア・ソフトウェアのみならず、それらを適切に運用・管理するために必要なすべての人や物を含んでいる。

---

27 http://www.bsi.org.uk/

28 http://www.fisc.or.jp/

一方、GMITS[29]は、IT セキュリティ・ポリシーを対象にしたガイドラインであり、IT セキュリティ・ポリシーとは「組織とその IT システムの範囲内で、重要情報を含む資産をどのように管理、保護、および分配するかを統制する規則、指令、および実践」と定義されています。

また、各省庁向けの「情報セキュリティポリシーに関するガイドライン[30]」（情報セキュリティコントロール推進会議）では、対象範囲を「ハードウェア、ソフトウエア、記録媒体等の情報システム等（システム構成図等の文書を含む。）及び全ての情報のうち、情報システムに電磁的に記録される情報、並びにこれらの情報に接する全ての者とする。」と定義しています。

このように、組織が所有する全ての情報を対象としているのか、あるいは情報システムで取り扱われる情報だけを対象としているのかといった点で各ガイドライン毎に情報セキュリティポリシーの守備範囲が若干異なっています。ただし、これは情報リスクマネジメントサイクルの対象範囲を、情報セキュリティポリシーに応じて狭めてよいということではありません。GMITS では、IT セキュリティ・ポリシーの上位ポリシーとして企業セキュリティポリシーがあることが前提とされています。また、これまで各部門毎にセキュリティ対策が行われてきた組織では、総務部から文書管理規程や設備管理規程、人事部から服務規程といった具合に、それぞれの部門の守備範囲毎に情報セキュリティに関する規則が発行されている場合も多いのではないでしょうか。

セキュリティポリシーを策定する際には、まずその対象範囲を明確にしなければなりません。そして次に、既存文書との関係を明らかにしなければなりません。最終的に情報セキュリティに関する全ての関連規則を総合的に俯瞰した時に、組織の全ての情報に対する保護対策が網羅されている必要があります。

そして、本来情報リスクマネジメントは、このように組織が所有する全ての情報を対象とした取組みのため、その守備範囲はとても広いものです。このような理由から、横並びの各部門で都度調整しながら進める方式ではなく、CIO あるいは CISO（Chief Information Security Officer：最高情報セキュリティ責任者）をトップに置いた情報セキュリティマネジメント体制を整備し、対策を進めた方がより潤滑に事が運ぶと考えられます。

本書では、対象者を情報システム部門の責任者に置いている点、また企業

---

29 http://www.iso.ch/

30 http://www.kantei.go.jp/jp/it/security/taisaku/guideline.html

が所有する情報のほとんどは、情報システムに関連している点を鑑み、特に情報システムに関連した情報リスクマネジメントの取組みを中心に紹介していきます。

3.2.2 情報セキュリティポリシーの構成

情報セキュリティポリシーの文書構成には、特に決まりがある訳ではありません。一般的には以下の 3 階層の文書構成をした情報セキュリティポリシーをよく見かけます。

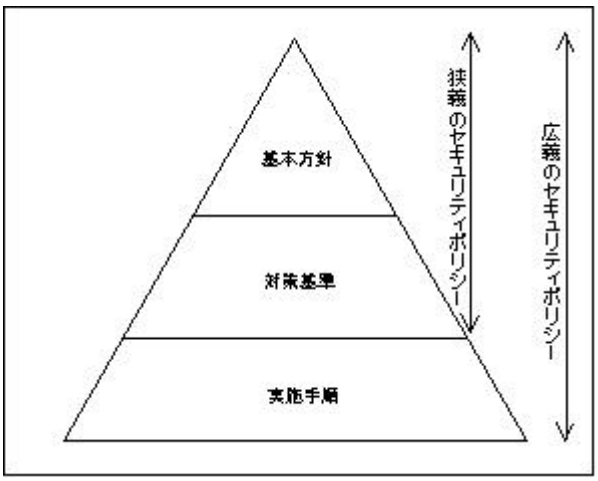

図 3-3　3 層構造の情報セキュリティポリシー

各階層の違いは、承認レベルや管理部門の違いと記述内容の具体性の違いです。基本方針で定められた内容が、下位の文書で段階を追って具現化されています。このトップダウン型の文書構成は、多くの組織の意思決定構造とも一致するため、採用されるケースが多かったのだと考えられます。

通常、基本方針や対策基準は組織の最終的な意思決定者である経営者レベルで承認され、情報セキュリティの全社的な組織であるセキュリティ委員会などで管理されます。一方、実施手順は情報システム毎、あるいは部門毎に作成・管理されることが多く、各部門の部門長が承認者であることが一般的です。

また、これとは違った文書構成の例として、対策基準と実施手順をまとめた内容の文書を、情報システム毎に策定する方法もあります。（図 3-4）これは、各情報システムの所管部署が大きく異なり、運用管理に関する共通のルールを策定することが難しい場合に有効な形式です。

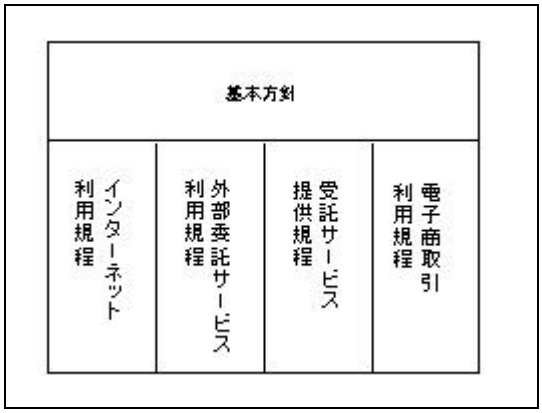

図 3-4 2 段階構成の情報セキュリティポリシー

この形式によるセキュリティポリシーでも、基本方針は役員レベルの承認とセキュリティ委員会などセキュリティ担当部門での管理が必要です。情報システム別のセキュリティポリシーは、各情報システムの所管部署の部門長の承認と所管部門の管理という形式が一般的になると思われます。

ここで、セキュリティポリシーという用語はしばしば多義的に使用されます。例えば、前出の 3 層構造の場合、基本方針と対策基準のことを総じてセキュリティポリシーと呼ぶ場合があります。また、ファイアウォールを始めとするセキュリティ製品の設定ルールがセキュリティポリシーと呼ばれることもあります。そして、これらセキュリティに関する文書を総体的に表す用語として、セキュリティポリシーが使用される場合もあります。
このように、組織のセキュリティ対策に関する意思が反映された文書は、その対象範囲や記述内容に関らずセキュリティポリシーと表現されることがあるので、その使用方法については留意しておかなくてはなりません。
本書では図 3-3 に示した 3 階層の情報セキュリティポリシーを前提として話を進めます。また、特に断りがない限り、情報セキュリティポリシーは基本方針と対策基準の両方を表す用語として使用します。

情報セキュリティポリシーに規定される内容についても、特にはっきりとした決まりがある訳ではありません。もちろん、その対象範囲によって記述される内容に違いが出てくることは言うまでもありません。技術的な対策だけでなく、人事面、設備面、環境面、契約面等の領域における対策についても網羅的に検討を行います。

（1）基本方針に記述される項目の例

一般に基本方針には、情報セキュリティに関する組織の取組み姿勢、および組織全体に関することについて記述します。また、対策基準で規定されていないケースが生じた場合の判断の拠り所となるのもこの基本方針です。

1. **声明**
2. **目的**
3. **情報セキュリティポリシーの位置付け**
4. **用語の定義**
5. **対象範囲**
6. **情報セキュリティマネジメント体制**
7. **準拠性**
8. **罰則**

（2）対策基準に記述される項目の例

対策基準では、基本方針の内容を受けて具体的なルールを記述します。各組織の業務形態やシステム形態、情報セキュリティポリシーの対象範囲や、既存文書との兼ね合いで記述項目は大きく変化します。一般的には以下ような項目が含まれる場合が多いです。

1. **情報の取扱い**
   情報の重要度区分と重要度に応じた情報の管理方法等について
2. **物理セキュリティ**[31]
   情報システムの設置条件や付帯設備等について
3. **要員セキュリティ派遣社員やアルバイトの管理、セキュリティ教育、啓発活動等について**
4. **技術セキュリティ**
   ○情報システムの管理者に要求される事項
   アクセス管理、ユーザ管理、ネットワークセキュリティ等について
   ○情報システムの利用者に要求される事項
   ウィルス対策、パスワード管理、行動規範等について
5. **情報システムの開発**
   情報システムを導入する際にセキュリティ上満足しなければならない

[31] **フィジカルセキュリティとも呼ばれる。**

調達要件、開発要件等について

6. **アウトソーシング**
   情報システムの開発や運用を外部委託する際のセキュリティ上の要件等について
7. **事業継続計画**[32]
   セキュリティ問題発現時の対応について
8. **変更管理**
   モニタリング、監査等について

対策基準にあたる文書は、複数作成される例も数多く見受けられます。例えば、情報セキュリティポリシーの対象者毎に対策基準を作成する方法（システム利用者セキュリティガイドライン、システム管理者セキュリティガイドライン等）や対策基準の各項目毎に文書を作成する方法（アクセス管理基準、ウィルス対策基準等）などが見受けられます。

本書では、情報セキュリティポリシーの具体的な策定方法については取り上げません。また、実施手順については 3.4 節で触れます。

[32] **コンティンジェンシープランとも呼ばれる。**

3.3 情報リスクマネジメントの計画（Plan）

情報セキュリティポリシーが策定されたら、情報リスクマネジメントサイクルの運用に取り掛かります。本節では、情報リスクマネジメントの計画フェーズで実践される様々な活動について検討を行います。

3.3.1 リスク分析

計画フェーズでは情報セキュリティコントロールの計画を立案します。ここで、実効性のあるセキュリティ対策を立案をするためには、組織が現在必要としているセキュリティ対策は何かを正確に把握しておく必要があります。

そこで、計画フェーズではまず始めにリスク分析を実施します。リスク分析とは、分析対象である資産が抱える脆弱性を明らかにすることによって、資産で発生する可能性のある脅威と、その発生確率や発生した場合の影響度等を評価する方法です。リスク分析の方法については、現在様々な手法が提案されています。ここでは、分析手法のうち最も一般的な方法である詳細リスク分析[33]について解説します。

[33] ディテールアプローチとも呼ばれる。

コラム１　リスク分析で利用される用語

（１）脅威とは

脅威とは、分析対象である資産に対して好ましくない影響を及ぼす事象のことを指します。例えば、GMITS では、脅威を環境的な脅威と人造的な脅威に分類しています。人造的な脅威は更に意図的な脅威と、偶発的な脅威に分類されています。また、別の分類方法としては、脅威をその性質から災害、故障、過失、犯罪の 4 区分に分類する方法もあります。

人造的脅威		環境的脅威
意図的脅威	偶発的脅威	
盗聴 改ざん 不正アクセス コンピュータウィルス 盗難 等	入力ミス データ削除 設定エラー 機器故障 等	地震 火災 洪水 落雷 等

表 3-1　脅威分類

（２）脆弱性とは

脆弱性とは、脅威を引き起こす原因となる事象のことを指します。分析対象によって存在する脆弱性は異なります。脆弱性が存在しなければ、対応する脅威も発生することはありません。また、脆弱性自体は分析対象に何ら被害を及ぼすものではありません。あくまでも、脅威が発生するための条件となるものが脆弱性です。

脆弱性：セキュリティホールが存在するバージョンの Web サーバを使用している。

脅威：Web ページの書換え、データ盗難

脆弱性：推測されやすいパスワードを使用している。

脅威：不正アクセス、パスワードの無断使用によるなりすまし

（３）リスクとは

リスクとは、脆弱性によって引き起こされる脅威の危険性を表す指標のことを指します。リスクは分析対象の資産価値、脅威発現の可能性、脅威発現時の影響度、脅威に対するセキュリティ対策等を総合的に勘案して決定されます。

詳細リスク分析は以下の 7 つの段階を経て実施されます。

① ステップ 1：レビュー境界の確立

詳細リスク分析では、はじめに分析範囲を決定します。例えば、どの業務を分析するのか、あるいはどの情報システムを分析するのか。また分析対象として人的リソースや建物、設備等も含むのか、といったことについて作業前に線引きを行っておきます。

② ステップ 2：資産の確認

次に、詳細リスク分析では、分析範囲に含まれる資産を洗い出します。洗い出される資産は、ハードウェアやソフトウェアに留まらず、文書や資金、サービス、企業イメージ等、企業にとって資産価値を有するものを網羅的に洗い出す必要があります。

③ ステップ 3：資産評価と資産間の依存関係の確定

ステップ 3 では、ステップ 2 で洗い出した資産が組織にとって有する価値を決定します。本来は、全ての資産を財務上の価値として判断することが望まれます。しかし、事実上不可能であるため、財務的に換算不可能な資産については、高、中、低などの重要性の程度で判断することになります。

また、資産単独の価値だけではなく、資産間の依存関係についても確認しておく必要があります。例えば、発売が既に終了しており入手が不可能なアプリケーションソフトを、購入金額や保守金額から資産価値を 10 万円と定めたとします。しかし、当該ソフトウェアからのみ読み出すことの可能な情報の資産価値が 1000 万円である場合、このソフトウェアの資産価値も必然的に高くなるはずです。

④ ステップ 4：脅威の評価

ステップ 4 では、資産に対する脅威の評価を行います。脅威の評価にあたっては、脅威カタログを利用することが効果的です。脅威カタログとは、脅威とその発生過程、及び脅威発生時の被害状況についてまとめられた 文書で、一般的な脅威カタログはセキュリティ関連文書やセキュリティ団体から発表されています。また、組織特有の脅威に対応するために、組織が独自に脅威

カタログを整備している場合もあります。脅威カタログから、脅威が発生した場合に影響を受ける資産と脅威の発生可能性について検討を行います。

⑤ ステップ 5：脆弱性の評価

ステップ 5 では、資産に存在する脆弱性について確認するとともに、その脆弱性によってどの程度容易に脅威が引き起こされるかについて検討を行います。

⑥ ステップ 6：既存／計画コントロールの確認

まだセキュリティポリシーの策定やリスク分析を実施していない企業であっても、通常は資産に対する何らかのコントロールが既に存在、あるいは計画中であるはずです。ステップ 6 では、これら既存の、あるいは計画中のコントロールをリストアップし、ステップ 5 までの分析結果と比較します。比較の結果、どのようなコントロールを追加、あるいは削除すべきであるのか、追加するコントロールが既存のコントロールにどのような影響を及ぼすのか等について検討を行います。

⑦ ステップ 7：リスクの評価

ステップ 6 までの作業結果を総合的に勘案して、分析対象の資産がさらされているリスクの評価を行います。リスクの評価手法については、様々な手法が提案されていますが、資産価値、脅威の発生確率と発生した場合の影響度、および現在実施されている対策をパラメータとした関数で表現することが一般的です。

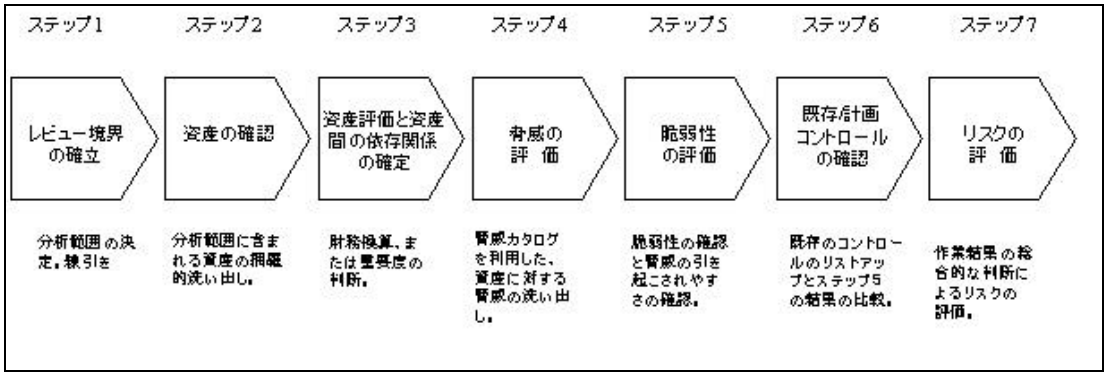

図 3-5　詳細リスク分析の流れ

詳細リスク分析では、厳密なリスクの確認に基づき適切なセキュリティ対策を実施することができます。反面、分析作業にはかなりの作業コストと専門知識が要求されます。そのため、企業が所有する全ての情報システムあるいは業務に対して、詳細リスク分析を適用することは現実的ではありません。その他のリスク分析手法については、第 4 章で解説を行います。

3.3.2 情報セキュリティ計画の立案

リスク分析の結果をもとに、組織に導入される情報セキュリティコントロールの計画を立案します。導入されるセキュリティ対策には、技術的な対策だけでなく、人事的な対策や、設備、環境面からの対策も含まれなければなりません。また、事前防止策だけでなく、セキュリティ問題の検出や回復等の事後対応策も考慮されていなければなりません。

情報セキュリティ計画の立案にあたって、他部門との調整や折衝を行う必要性があるかもしれません。例えば、情報システム部門以外で導入しているサーバがインターネットに直接つながっており、組織全体の情報資産が脅威にさらされていることが判明したとします。該当システムに対して、物理的な設置場所はどこであるべきか、システム管理者権限は誰が所有すべきか、インターネットとの接続口に設置するファイアウォールの購入費用はどの部署が負担するのか等、多くのことを決定しなければなりません。また、その決定は情報システム部門だけではなく、該当部門にも納得して受け入れてもらえなくてなりません。例えば、新規のセキュリティ対策を導入した結果、情報システムの使い勝手が変化したとします。この変化を、情報システムのユーザに受け入れてもらうためには時間的コストが発生します。リスク分析の結果を忠実に対策として反映しようとすると、思いのほかセキュリティ対策のコストがかかることが実感されるでしょう。

「KPMG Information Security Survey 2000 Report(2000 年 12 月発行)」[34]の調査結果より、1999 年度及び 2000 年度に組織が情報セキュリティコントロール費用として確保した予算を図 3-6、3-7 に示します。調査結果より、

---

[34] 「KPMG Information Security Survey 2000 Report （2000 年 12 月発行)」日本国内売上高上位 3500 社及び中央官庁、地方公共団体、公益法人等合計 3700 社を対象に郵送により実施。有効回答数は 410 組織。（KPMG ビジネスアシュアランス株式会社）
http://www.kpmg.or.jp/whatsnew/whatsnew05.htm

セキュリティ対策費用として 1000 万円を超える投資を行っている組織が 1999 年度では 24 組織でしたが、2000 年度では 36 組織に増加しています。しかし、セキュリティ対策費用が 200 万円に満たない組織も過半数の 79 社を占めており、セキュリティ対策のために、十分な投資とリスク分析を行っている組織はまだまだ少ないと推察されます。

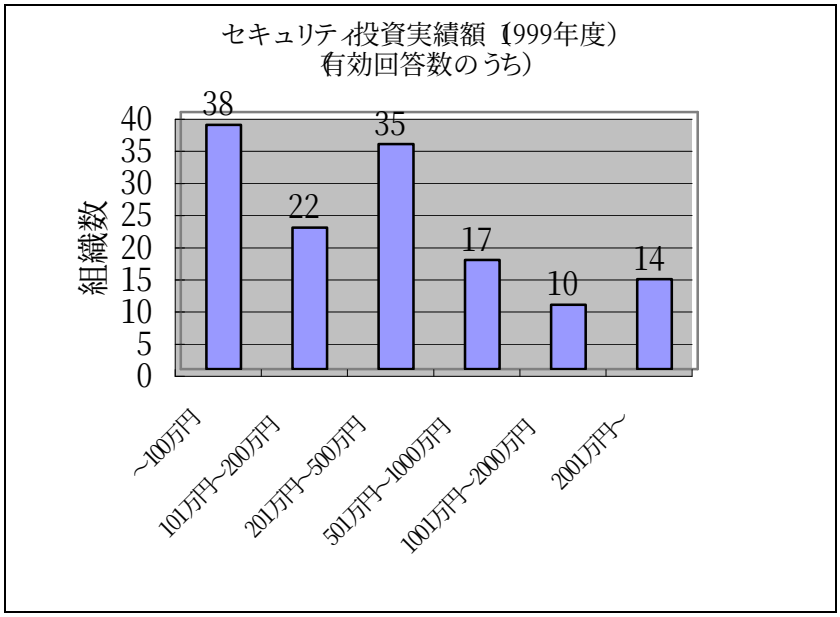

図 3-6　セキュリティ投資予算額（1999 年度）

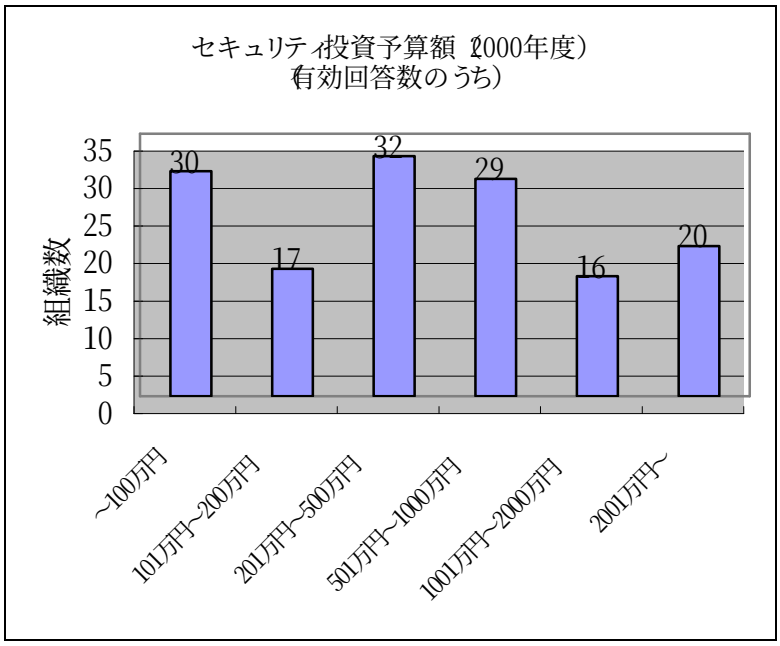

図 3-7　セキュリティ投資予算額（2000 年度）

（1）リスク受容[35]

ここで、セキュリティ対策に十分な投資を行うことは重要ですが、リスク分析の結果、明らかになったリスク全てに対策を実施することは、大抵の組織においては現実的ではありません。実際には、対策を実施するリスクに一定の閾値を設け、ある大きさ以下のリスクに対しては、対策の実施を見送るケースも多々発現します。この考え方をリスク受容と呼びます。

リスク受容とは、ビジネスを進めるにあたって、実施するセキュリティ対策の規模を検討した結果、対策を見送ったリスクがあることを認識し、そのリスクを受け入れることです。あくまでも、リスクを承知した上で容認することを指し、認識していないリスクが存在することはリスク受容とは呼びません。

企業が利益を獲得していくためには、容認できるリスクレベルを設定し、そのレベルまでリスクを低減するためのセキュリティ対策を実施し、容認レベル以下のリスクに対してはリスク受容しながら企業活動を行っていかなければなりません。そして、そのためには、自社におけるリスクの評価手法とリスクの容認レベルを確立しておく必要があります。

企業は、ビジネスにおけるリスクを正しく評価した上で、リスク受容を行って該当ビジネスを継続するのか、あるいはリスクを回避しビジネスを行わないという選択をするのか、という経営判断を行う必要があります。これは経営者だけではなく、情報システム部門の責任者にも当てはまることです。情報システム部門の責任者は、常に獲得した予算でどの範囲のシステム開発投資を行うのか、どの範囲でセキュリティ対策を行うのか、教育費用にはいくらかけることが可能なのか、といった判断をする必要があります。

---

35 **リスクテイクとも呼ばれる。**

コラム２　ランニングコストの考え方

ある情報システム部門の部門長が、初めてセキュリティ対策予算を次年度予算に計上した際に、所管役員から「今まではセキュリティ対策を行っていなかったのか、それは会社に損害を与える職務怠慢行為ではなかったのか。」と詰問されました。今まではシステム管理費用の一部でセキュリティ対策を行っていたのであって、無策だったわけではないと回答したところ、次年度以降もそうすればよいといって予算を削られてしまいました。また、現場部門のシステム担当者がセキュリティ対策のための予算の獲得を上司に相談した際にも、先程の部門長と同様のことを言われて予算獲得を断念せざるを得なくなってしまいました。彼らの経験は決して珍しいことではなく、セキュリティ対策予算を獲得しようとすると誰もが直面する可能性のある出来事です。

多くの情報システム部門の責任者が、セキュリティ対策予算の確保にあたっては、まず始めに機器購入などの外部に資金が流れる部分のみを予算化し、人員のやりくりは内部で何とかしようと考えるようです。そして、次ステップに進もうとした段階でこのような反発に合い、それ以上の活動が取り止めになってしまうことが少なくありません。

しかし、組織全体の情報リスクマネジメントと、個別問題に対応するセキュリティ対策では目的も効果も必要なリソースも全く異なります。特に、セキュリティ教育・啓発活動を行うためには、情報システム部門以外の人間の時間も取られるということを忘れてはなりません。情報リスクマネジメントのランニングコストとして、情報システム部門で消化される経費や人件費のほかに、他部門の人員の人件費も必要なのです。

はじめから大上段に構えた情報リスクマネジメントを導入することが難しい場合、組織のセキュリティに対する意識を少しずつ高めてから移行していくことも時には必要です。しかし、この場合は手遅れになるかもしれない危険性を認識し、一定のセキュリティレベルが確保されているならそれ以上を行う必要はないのではないか、という内部からの反発を説得する材料を用意しておかなければなりません。

事例５　セキュリティポリシー作成のきっかけ

「KPMG Information Security Survey 2000 Report(2000年12月発行)」の調査結果によると、2000年秋時点で約3分の1の組織がセキュリティポリシーを導入していました。

しかし、一口にセキュリティポリシーと言ってもその内容にはばらつきがあり、コンピュータウィルス、インターネット、ネットワークといったキーワードは項目として定められているものの、その他の基本的項目（セキュリティ組織と管理、情報分類等）を定めている組織は7割程度でした。また、ソフトウェアのライセンス管理や情報セキュ

リティ教育に対する規程を持つ組織は更に少なく、ビジネス継続計画を定めている企業に至っては全体の約2割程度でした。この結果は、セキュリティポリシーを導入したきっかけも大きく影響していると思われます。

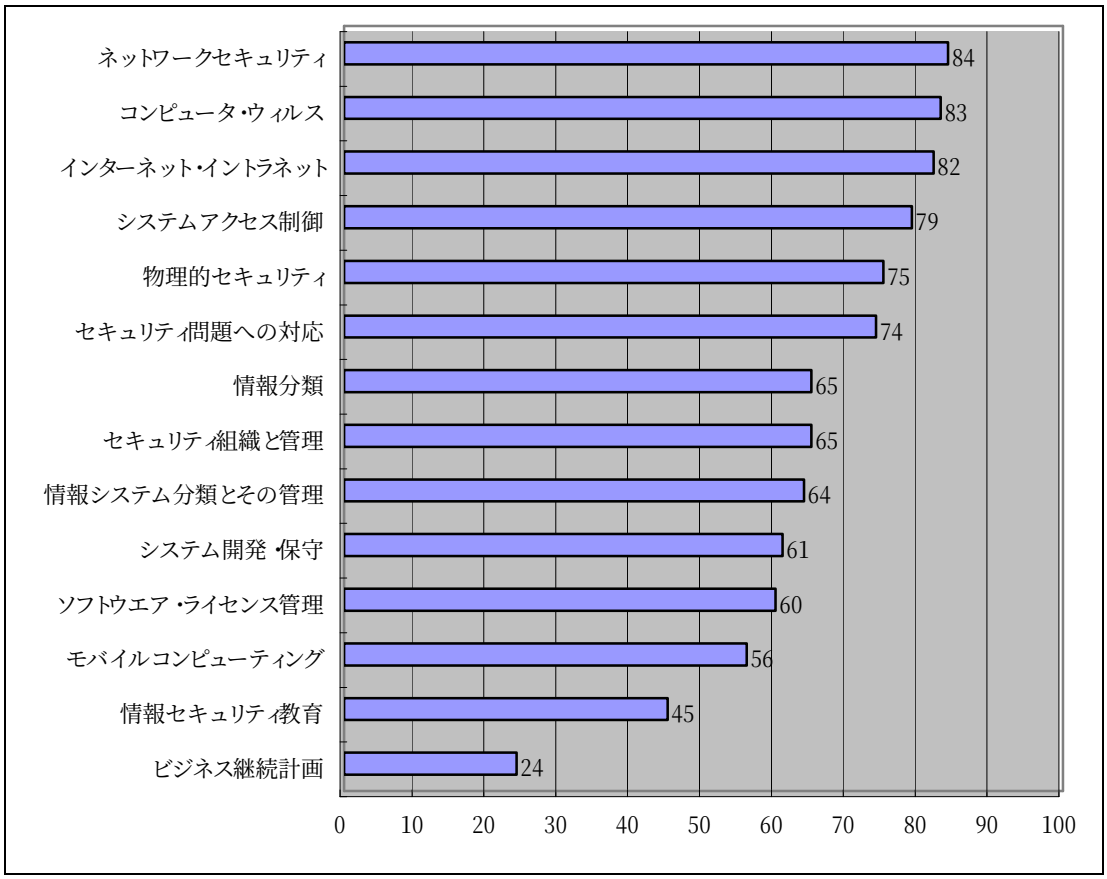

図3-8　セキュリティポリシーの対象項目

セキュリティポリシー導入のきっかけは、「外部要因」と「内部要因」に分けることができます。外部要因とは、取引先企業からセキュリティポリシーの提示を求められる、業界団体がセキュリティポリシーの策定を業界方針として決定する、監督省庁からの指導、親会社のセキュリティポリシーをグループ企業に展開することになり対象になった、といったことが考えられます。内部要因としては、セキュリティ意識が高まり必要性が現場から持ち上がった、IR活動の一環としてセキュリティ対策を宣伝することになった、セキュリティ事故が発生したため対策を取らざるを得なかった、といったことが考えられます。しかし、外部要因によってセキュリティポリシーを導入する場合は、概して導入期間が短く、特に取引先企業から提示を求められた場合などは、1ヶ月程度でただ文章を作文したというレベルのセキュリティポリシーを全社規程としてしまった組織もあります。自社はもうセキュリティポリシーを導入しているから大丈夫、と安心せずに情報リスクマネジメントサイクルを適切に運用し続けることが肝心です。

3.4 情報リスクマネジメントの実施（Do）

情報リスクマネジメントは、何らかの機器やシステムを導入すればそれで全ての問題が片付く、というわけにはいきません。2000 年初頭に、省庁のホームページの改ざんが相次いだ際、マスメディアはまるでファイアウォールを導入してさえいれば、全ての問題が回避可能であったかのような報道をしました。しかし、現実は大きく異なります。ファイアウォールの導入だけを取り上げたとしても、誰がファイアウォールの設定変更をする権限があるのか、誰がアクセスログを分析するのか、どういった体制でネットワークを管理するのか、といった問題を解決していかなければなりません。またファイアウォールの実運用にあたっての手順書、利用者マニュアルも整備しなければならないのです。本節では、情報リスクマネジメントの実施フェーズで実践される様々な活動について検討を行います。

3.4.1 情報セキュリティマネジメント体制の整備

情報リスクマネジメントの実施フェーズの第一歩として、多くの情報セキュリティの参考書には「全社的にセキュリティを統括する情報セキュリティ委員会を作るように」と書かれています。事実、多くの組織がセキュリティ対策の実施主体として情報セキュリティ委員会を設置しています。

しかし、当然のことですが、委員会を組織し、委員を任命したとしてもそれだけで全社的なセキュリティ管理体制ができるわけではありません。情報リスクマネジメントに関わる関係者の責任、権限と義務を明確化し、それぞれの関係者が適切な統制を受けなければ、組織として委員会があっても何の役にも立ちません。更に言えば、改めて委員会組織を整備する必要は必ずしもないのです。セキュリティポリシーや就業規則などで情報リスクマネジメントのあり方が明確に規定されており、各人がどのように行動すべきかが明確でありさえすれば、既存の委員会や会議に新たな職掌として情報リスクマネジメント上の役割を割り振るだけでも何ら問題はありません。

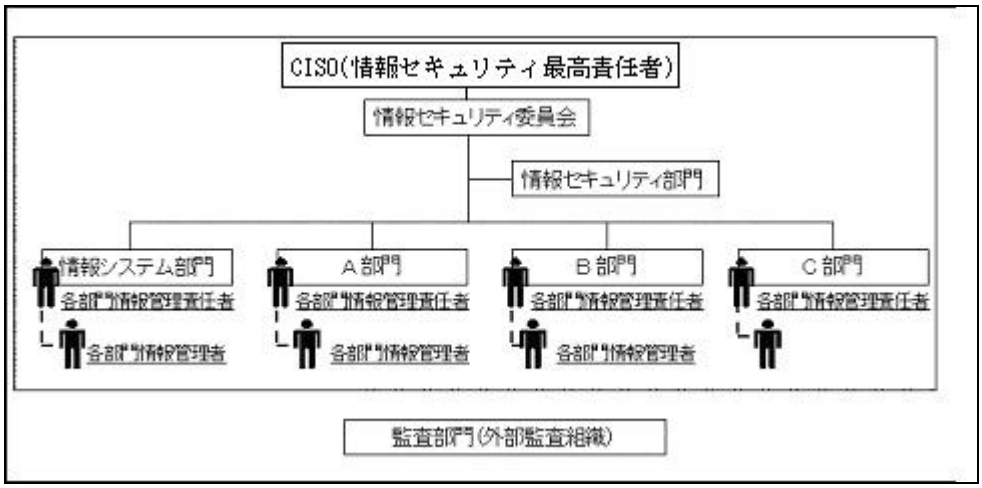

図 3-9　情報セキュリティマネジメント組織例

3.4.2 実施手順の整備

実施手順とは、情報セキュリティポリシーを組織に導入するために必要となる文書の総称です。具体的には、操作・運用マニュアルや利用者ガイドライン、業務手順書、実施計画書、申請用紙、管理台帳等が該当します。

実施手順は、情報セキュリティポリシーの記述内容の詳細さやその他のセキュリティ関連の既存文書の整備状況等に応じて、各組織毎に必要となるものが異なってきます。情報セキュリティポリシー導入のために必要な実施手順は、以下の 3 つの観点をもとに策定されます。

① 情報セキュリティポリシーによって新しく定められた業務手続き

情報セキュリティポリシーの策定により、新たな業務手続きが生じる場合があります。これらの手続きについては、既存の関連文書等が存在しないため、新規に運用手順書を作成する必要があります。

② あいまいな記述の具体化

情報セキュリティポリシーでは、汎用性を確保するためにあいまいな記述を採用する場合があります。あいまいな記述については、システムや各部門の状況に応じて、具体的な解釈を行う必要があります。

③ 理解・浸透の促進、重点ポイントの強調

基本方針及び対策基準に規定された内容のうち、特に強調したい事柄については、別途解説書やガイドラインとしてまとめると効果的です。

実施手順は、その文書の性質によって、作成する主体も情報システム部門や情報システムの管理者、あるいは各部門の責任者であったりと様々です。また、実施手順を整備していく過程で、各自が自身に関連するポリシーを理解し、実践していくことも副次的な効果として期待されます。

3.4.3 情報セキュリティ教育

情報リスクマネジメントを実践し、成果を上げるためには、情報セキュリティの重要性を関係者が十分に理解し、自分の行動がどのような影響をもつのかを認識した上で、主体的に情報セキュリティの確保に協力することが必要です。そのためには、関係者への動機付けが重要です。特に、情報セキュリティポリシーが作成された後に一方的に遵守するようにと要求された関係者にとっては、強い動機付けがなければなりません。

関係者に情報セキュリティポリシー遵守の動機付けを与える手段の 1 つが、情報セキュリティ教育です。情報セキュリティ教育の実施方法としては、

- 説明会の開催
- 社内研修への組込み
- 社外講師を招いての講習会の開催
- イントラネットや電子教材を使ったセルフラーニング

等が考えられます。どれか 1 つの方法のみを採用するのではなく、組織の実状にあわせて適切な方式を組み合わせる必要があります。また、セキュリティ教育活動は、ポリシーの初期導入研修、ポリシーで規定された役職別研修、組織内の情報リテラシーの高まりに併せたテーマ別講習等、複数の教育内容を用意しておかなければなりません。

◯セキュリティ教育プログラムの例

- セキュリティポリシー説明会
- システム管理者説明会
- 情報セキュリティ責任者説明会
- 不正アクセス対策説明会
- コンピュータウィルス対策
- 情報セキュリティ関連法規講習会

- ネチケット[36]講習会 等

情報リスクマネジメントでは、情報セキュリティ教育を軽視することができません。セキュリティ教育は、時間的コストが嵩みます。しかし、セキュリティ教育を実施することで、全社的な情報リテラシーを高める効果も期待できます。セキュリティ確保という守りの姿勢としてだけではなく、全社的な情報リテラシーの底上げという積極的な側面からも、セキュリティ教育の実施は企業にとって不可欠です。

3.4.4 情報セキュリティ啓発活動

情報リスクマネジメントでは、教育活動と同じく啓発活動も大切です。教育活動ではどうしても「○○○しなければならない。」や「○○○をしてはならない。」といったお仕着せのスタイルに成りがちです。そこで、啓発活動を行うことによって、「情報セキュリティは大切」である、という雰囲気作りを併せて行っていくことが情報リスクマネジメントを組織に浸透させるためには必要です。代表的な啓発活動としては、以下の 7 つの活動が考えられます。

① イントラネットサーバへのセキュリティ関連情報の掲載
② 情報セキュリティに関するパンフレットの作成、配布
③ 情報セキュリティに関するポスターの作成、掲示
④ 定期的なニューズレターの発行（毎回異なる情報セキュリティのトピックを取り上げ詳細に説明する。）
⑤ 情報セキュリティに関するビデオ教材の作成、活用既存の周知方法の利用
⑥ 情報セキュリティに関する自己評価アンケートの実施

啓発活動にあたっても教育活動と同様に、複数の方法を織り交ぜ、繰り返し実施することが必要です。また、教育プログラムとも連携させる必要があります。今まで、情報セキュリティの教育、啓発活動は軽視されてきました。効果が見えにくく、対費用効果を測定することが難しいため、情報リスクマネジメントにおいて、最も予算を獲得しにくい分野のひとつといえるでしょう。しかし、情報リスクマネジメントにおいて最も有効な手段が、教育・啓発活動です。2 章で紹介したような手法を使って、セキュリティ教育活動の

---

[36] Internet など、ネットワーク上でのやり取りにおけるエチケットやマナーを指す言葉で、「ネットワーク」と「エチケット」からの造語。

有用性を可視化し、積極的に取り組んでいかなければなりません。

3.4.5 モニタリング

情報リスクマネジメントを実践するためには、常に変化しつづける脅威に対応するために、定常的にビジネス環境を監視し、その状況を常に把握し続けなければなりません。この取組みをモニタリングと呼びます。

モニタリングの例① セキュリティ情報の収集

セキュリティ情報の収集とは、情報システムのセキュリティ情報を定常的に収集管理する活動のことを指します。例えば、情報セキュリティコントロールとして導入した情報機器に重大な欠陥が見つかったとします。このような情報はメーカーからの連絡を待っているのでは対応が遅れ大きな被害を被ります。担当者を決め、組織内で重要な情報機器については常にホームページやメーリングリストなどからセキュリティ情報を収集しつづけることが必要です。そして、脅威が発生すると同時に組織に与える影響度を的確に判断し、対応しなければなりません。また、サーバのアクセスログの監視もこの種のモニタリングに分類されます。

モニタリングの例② 構成管理

構成管理とは、情報システムの構成を定常的に管理する活動のことを指します。ビジネス環境は時々刻々と変化していきます。そして、情報システムもまた変化するビジネス環境に対応するために、導入後も絶えず構成変更がなされていくものです。そして、情報システムの構成変更の都度、新たなリスクが発生しているとも考えられます。情報システムの構成管理はモニタリングにおける最も基本的な作業です。情報システムを介さない部分の業務手続きの手順変更に関する監視もこの種のモニタリングに分類されます。

モニタリングの例③ 資産価値の管理

資産価値の管理とは、情報システムの資産価値を定常的に管理する活動のことを指します。例えば、セキュリティポリシーの導入時は組織メンバーのITリテラシーが低くほとんどイントラネット掲示板が利用されていなかった組織が、その後の熱心な啓発活動で情報ネットワークを利用した情報共有が

盛んになり始めたとします。情報機器構成は変化していなくとも、共有ファイルサーバには今まで紙で保管されていた営業提案書や契約書が保存されるようになり、電子メールのトラフィックも増大したとします。この場合は、情報の価値に見合ったコントロールの変更、ネットワーク回線の増強などの対応が求められます。

モニタリングの例④ 利用状況の管理

利用状況の管理とは、情報システムの利用状況やユーザの情報リテラシーを定常的に管理する活動のことを指します。例えば、パソコンの利用を開始した当初は、ウィルスチェックソフトを利用者が各自で実行することが不可能であったため、各グループで責任者を決めてその人がグループ内の全パソコンのウィルスチェックを行っていたとします。しかし、数ヶ月もしないうちに全員がウィルスチェックソフトを起動させ、ウィルスチェックを行うことができるようになったとします。この場合、一人の人間の不在がグループ内の全パソコンがウィルス感染の危険性を引き起こすような仕組みは早急に解消し、一人一人がウィルスチェックを実行するように、コントロールを変更すべきです。資産価値の管理とは、資産価値に変化が生じない点で異なっています。

社外からの要請	取引開始に際し新たなセキュリティ要件が発生した。
社内の状況変化	採用したセキュリティポリシーが厳し過ぎ、業務の実態にそぐわない。 遵守可能な範囲から採用した最小限のセキュリティポリシーが浸透し、さらにセキュリティレベルを上げる余裕ができた。 社内で大規模なシステムの再構築を行った。
外部の環境変化	脅威が増大した。 脅威が減少し、対策費用が見合わなくなった。

表 3-2　ビジネス環境の変化の例

表 3-2 にモニタリングによって検出されるべき、主要なビジネス環境の変化をまとめます。表 3-2 のような事象が報告された場合には、導入されているコントロールの見直しを行わなくてはなりません。

3.5 情報リスクマネジメントの評価・見直し（See）

本節では、情報リスクマネジメントの評価・見直しフェーズで実践される様々な活動について検討を行います。

3.5.1 情報セキュリティ監査

情報リスクマネジメントが的確に機能しているかどうかを確認するためには、定期的に情報セキュリティ監査を行わなければなりません。

情報セキュリティ監査の目的は大きく 2 つあります。1 つ目の目的は、情報セキュリティポリシーが遵守されているかどうかを確認することです。インタビューや書類調査、現状視察などによって、情報セキュリティポリシーの組織への浸透度測定や、現在実施されているコントロールの情報セキュリティポリシーへの準拠性に関する調査を行います。

2 つ目の目的は、現在実施されているコントロールが有効に機能しているかどうかを確認することです。導入したコントロールが形骸化していないか、あるいは、コントロールがビジネス環境や情報技術の変化に適応できているか等、コントロールの有効性と妥当性に関する調査を行います。

（1）侵入テスト[37]

ここで、特に 2 つ目の目的であるコントロールの有効性を確認する手段の 1 つとして侵入テストを挙げることができます。[38]

侵入テストとは、侵入者が用いる手法を実際に試み、その結果によってコントロールの有効性を確認する監査手法です。侵入テストには、ツール等を用いたセキュリティホールの検出テストと、ソーシャルエンジニアリングを用いた管理体制のテストの 2 つの手法があります。

セキュリティホールの検出テストでは、セキュリティホール検出用ツールあるいは、インターネット上で公開されているクラッキングツールを用いて技術面のコントロールの有効性を検査します。セキュリティホール検出テストでは、情報システムに悪影響を及ぼす可能性があるため、実施時期と問題が発生した場合の対処方法をあらかじめ明確にし、関係者に周知した上で実施しなくてはなりません。

---

37 ペネトレーションテストとも呼ばれる。

38 「インターネットセキュリティ」Larry J Hughes, Jr.（インプレス）1997 年

管理体制のテストでは、ソーシャルエンジニアリングと呼ばれる人間の接触を伴う手法を用いて、管理面のコントロールの有効性を検査します。ソーシャルエンジニアリングの代表的な手法としては、関係者を装って電話をかけパスワードを聞き出したり、清掃員になりすましてオフィスに侵入し情報を収集したりするような方法があります。詳細はコラムを参照してください。

情報セキュリティ監査の結果は、経営者に提出され、その後監査結果を反映した適切な対策を実施することになります。情報セキュリティ監査は、情報セキュリティポリシーの全項目に関して実施する場合と、ある特定のテーマ（例えばコンピュータウィルス対策、不正アクセス発生時の対応、情報分類と情報管理の適切性等）を設定して、実施する場合があります。計画フェーズで、情報セキュリティポリシーの導入計画に合わせて、監査テーマと監査対象及び監査実施時期を立案しておくことが望まれます。

（2）外部監査と内部監査

監査は、その実施主体が自組織か外部組織かによって内部監査と外部監査に分けられます。通常、監査結果の客観性を保つために、情報セキュリティ監査を実施する人間は、監査対象となる情報システム（あるいは業務）の運用管理に携わっていない人間でなければなりません。しかし、情報セキュリティに関して必要な知識、技術及び経験をもった人材でなければ、情報セキュリティ監査を行うことはできません。情報セキュリティ監査が可能なスキルレベルを有した人材は情報システムの運用管理に従事していることが多く、年数回の情報セキュリティ監査のために、専門の人材を組織で確保することはあまり効率的ではありません。以上の理由から、会計監査のように法的拘束は無いものの、情報セキュリティ監査にあたっても、外部監査を受けることが望ましいと考えられます。

侵入テストを含む情報セキュリティ監査を行うことで、実施されているコントロールの問題点が把握できるだけでなく、情報セキュリティに関するレビューによって、組織内でセキュリティ意識が高まり、情報リスクマネジメントが有効に機能するよう働きかけることが可能になります。

3.5.2 情報セキュリティコントロールの見直し

モニタリングや情報セキュリティ監査を通じて、何らかの問題が発見された場合、情報セキュリティコントロールの見直しを行う必要があります。実際には、発見された問題に対してリスク分析を実施し、リスクのビジネスへの影響度合いによって優先順位をつけてから、情報セキュリティコントロー

ルを実施することになります。

情報セキュリティコントロールの見直しの後は、再び計画フェーズに戻ります。もちろん、見直しの結果、計画フェーズへ遷移する前に、情報セキュリティポリシーの改訂作業を行わなければならない場合もあります。情報リスクマネジメントサイクルは、基本的にはシステム監査のタイミングに合わせて、1 年に数回循環します。また、新しいセキュリティ問題が見つかった場合等は部分的に小さく循環することもあります。

そして、情報リスクマネジメントサイクルは、同じ輪の上で周り続けるのではなく、徐々に輪が上昇し、セキュリティレベルが向上し続ける（=スパイラルアップする）ように運用しなければなりません。

コラム３ システムの外部監査

「2000年システム監査白書」(システム監査学会/日本情報処理開発協会)によると、上場企業のシステム監査の実施率は1998年に20.4%、1999年に34.2%と実施率自体は上昇傾向にあることがわかります。しかし、トップマネジメントがシステム監査対象を決定する企業は、監査実施企業全体の10.4%、またシステム監査テーマを決定するのは8.5%にすぎません。つまり、システム監査を実施していてもマネジメント層が関与しておらず、この状況では改善勧告の円滑な実施は難しいと言えるでしょう。

情報リスクマネジメントのSeeのフェーズとして、外部監査は有効です。しかし、外部監査サービスを提供する企業に全てをまかせ、監査報告書を読むだけは外部監査のメリットを享受できません。外部監査を実施するのは、組織と関連のない団体ですから、大きなシステム改善やセキュリティ問題の発生といった事実を彼らは知り得ません。適切な監査を実施するためには外部監査において特に重視するテーマを定める等、組織内部の人間の協力が必要なのです。特に、組織戦略に関わる大きなリスクが発生している可能性に最も敏感になるべきトップマネジメントの積極的な関与が望まれます。

コラム４　ソーシャルエンジニアリング

ITT技術の名称ではなく、「信用詐欺」と呼ばれてきた、心理的誘導によって自分の欲する情報を提供させる技術です。電話やEメールで他人になりすまし、本来アクセス権限のない情報を聞き出したり、相手に自分を信用させて直接情報を収集したりするといった、システム面では防ぐことのできない情報操作・収集方法であるため、防止には情報を取り扱う全関係者に対する教育・セキュリティ啓蒙活動が重要視されます。

ゴミ袋から拾われたインターネットプロバイダの請求書の情報を元に現行よりも有利な契約体系を勧め、一旦相手の信用を得てから「今すぐ有利な契約内容に以降するための設定変更に必要」と言ってパスワードを聞き出す、といった物理面と心理面を組み合わせた犯罪が発生した例があります。これは個人ユーザが対象となりましたが、犯罪者がASPのフリをして同様の電話をかけてきた場合、あなたの会社は「絶対に大丈夫」と言えるでしょうか。また、ゴミの捨て方などの物理セキュリティ対策は総務が、パスワードの管理などのITセキュリティ対策はシステム管理部が独自に行い、ASPとの契約は各事業部が独自に行っているという企業がこういった犯罪の対策を取ろうとする場合、責任の所管はどこにあると考えるべきなのでしょうか？

こうした複合的かつ巧妙な犯罪に対する対策のためにも、セキュリティ対策は全社的かつ全体的な視点と、セキュリティを所管する組織の明確化が必要なのです。

3.6 セキュリティインシデントへの対応

これまで､情報リスクマネジメントサイクルの各フェーズにおける様々な取組みを紹介してきました。これらの取組みはいずれも平時における取組みです。では、セキュリティ問題が発生した場合にはどのように対処すればよいのでしょうか。基本的には、セキュリティ問題への対応に関しても平時と同様 PDS サイクルに沿ったを運用しておくことが求められます。この件は、「CSIRT 体制と効果的なインシデント対応についての啓発コンテンツ[39]」で詳しく取扱います。

[39] IPA ISEC(IPA セキュリティセンター)　http://www.ipa.go.jp/security/index.html

3.6 情報リスクマネジメントサイクルの成功要因

図 3-10 に、情報リスクマネジメントサイクルの各フェーズで実施する活動を示します。

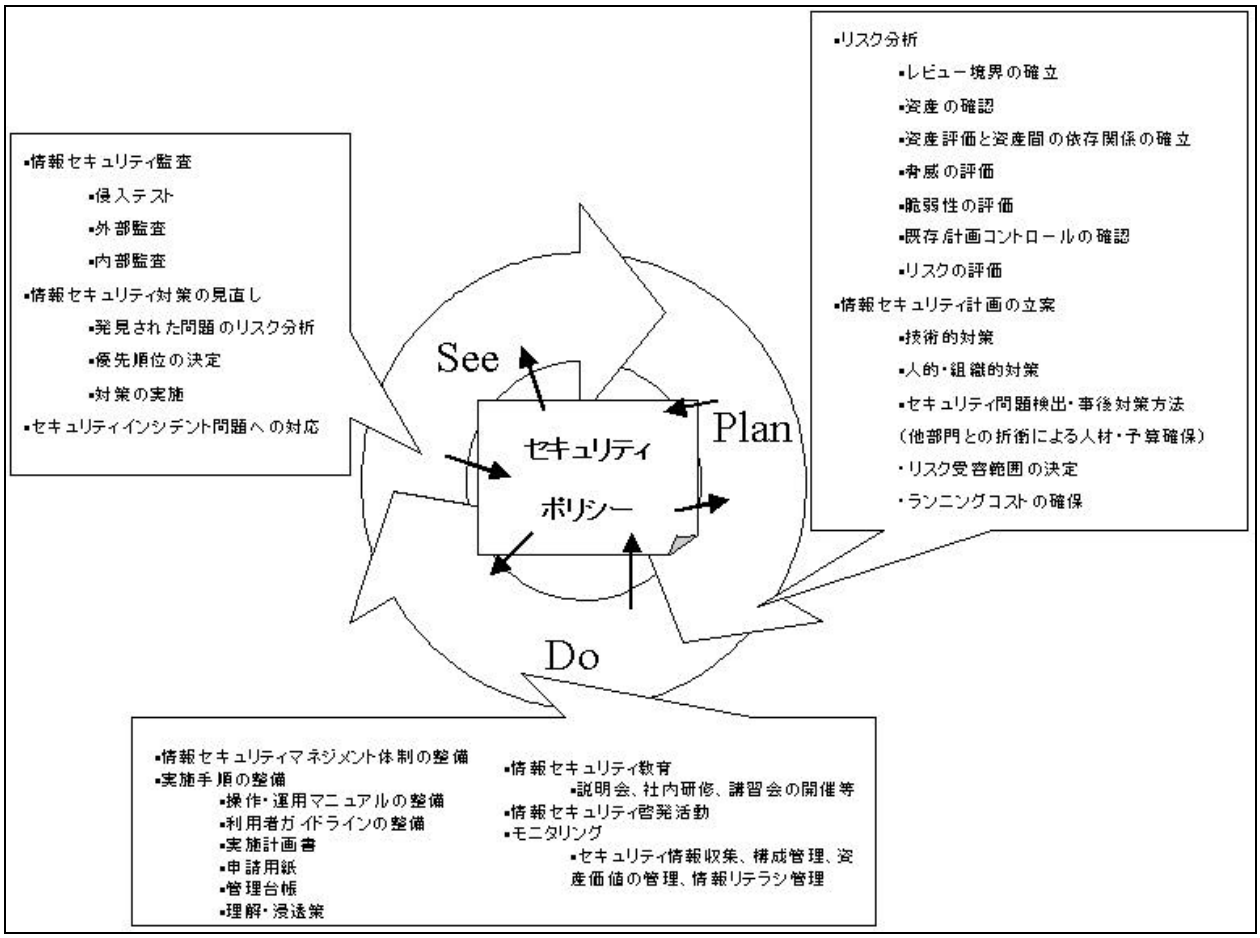

図 3-10　情報リスクマネジメントにおける作業例

フェーズ毎に大変な作業量があり、経営陣を始めとする全社的な協力体制のもと、十分なリソースを確保した状態でないと、サイクルの運営は難しいということが再確認されるのではないでしょうか。

ここでは、第 3 章のまとめとして、情報リスクマネジメントサイクルを成功させるための 5 つの要因について検討を行います。

1	情報セキュリティポリシー	事業目的を反映した情報セキュリティポリシー
2	情報セキュリティマネジメント体制	組織文化と整合性のとれた情報セキュリティマネジメント体制
3	情報セキュリティ教育	継続的なセキュリティ教育活動
4	経営者の意識	経営層の情報セキュリティマネジメントへの関与
5	十分なリソース	情報リスクマネジメントを達成するために必要なリソースの確保

表 3-3　IT リスクマネジメントの成功要因

情報リスクマネジメントサイクルの成功要因の 1 つ目は「情報セキュリティポリシー」です。情報セキュリティポリシーなくして情報リスクマネジメントを実施することはできません。また、実態と乖離した実効性を伴わないポリシーでは、情報リスクマネジメントサイクルも立ち行かなくなります。各組織の実状を反映した実効性のあるポリシーを策定しなければなりません。

成功要因の 2 番目は「情報セキュリティマネジメント体制」です。CISO を頂点としたトップダウンの管理体制を整備するとともに、対象者個々の責任を明確化することが望まれます。

成功要因の 3 番目は「情報セキュリティ教育」です。情報リスクマネジメントのサイクルをスパイラルアップさせるためには、組織に情報文化を根付かせ、セキュリティ意識の底上げをしていくことが必要不可欠です。

そして、情報リスクマネジメントサイクルを運営するための土台となるのが成功要因の 4 番目「経営層の関与」であり、成功要因の 5 番目「十分なリソースの確保」です。情報リスクマネジメントは「組織のセキュリティ目標」を達成するものなので、経営層の関与が不可欠です。情報システム部門の責任者は、経営層のセキュリティ意識を高める役割も担っているのです。また、情報リスクマネジメントの導入によってもたらされる膨大な作業量を消化するためには、それに見合ったリソースが必要です。情報リスクマネジメントサイクル運営のための十分なリソースを確保することが、情報システム部門責任者の最大の作業になるのではないでしょうか。

近年、情報セキュリティへの関心が集まり、部分的なコントロールはこれまでも実施されてきました。しかしこれらのコントロールが、情報リスクマネジメントという視点から見た時に有効性があるものなのか、そして妥当性があるものなのかもう一度見直す必要があります。現在実施しているコントロールを十分なものだと思い込まず、情報リスクマネジメントサイクルに沿って、継続的に運用管理していくことが求められます。

4 情報セキュリティに関する国際的ガイドライン

ビジネスを取り巻く環境が比較的均質であった既存の国内取引では、従来の商慣習に従うことでリスクを低減することが可能でした。しかし、インターネットの発達等の要因により、電子商取引をはじめとする海外とのビジネスが近年より活発になってきています。ビジネス環境が大きく異なる海外市場との取引では、既存の知識や経験だけでは予測不可能なリスクがあるかもしれません。このような状況下では、情報セキュリティに関する国際的なガイドラインへの準拠性を謳うことで、自らの安全性をアピールすることが効果的です。本節では、情報セキュリティに関する国際的なガイドラインについて解説を行います。

4.1 GMITS（ISO/IEC TR 13335）

4.1.1 GMITS の構成

GMITS は、IT セキュリティの管理に関する一般的なガイドラインを提供している国際標準規格です。（図 4-1）GMITS では、電子媒体による情報及び情報機器に対する概念的なマネジメント・プロセスを対象としており、非電子媒体はその対象となっていません。2001 年 1 月現在、4 部構成の本文と付録から構成されています。今後第 5 部としてネットワークセキュリティマネジメントに関わるガイドラインが提供される予定となっています。

第1部　IT セキュリティの管理に関する基本的な概念およびモデルの説明がなされています。組織の情報セキュリティに関する責任者が、情報リスクマネジメントに対する包括的な知識を獲得するために有用な資料です。

第2部　セキュリティマネジメントとセキュリティプランニングに関する説明がなされています。情報システムの調達、開発、運用等の活動に関する責任者やユーザ部門の責任者が具体的にコントロールを計画、実施するために有用な資料です。

第3部　セキュリティマネジメントの具体的な手法に関する説明がなされています。情報システム関連のプロジェクトの全体管理（プロジェクトマネジメント）を担当する人が実践すべき管理手法を検討するた

めに有用な資料です。

第4部　セキュリティマネジメントにおけるコントロールの詳細な説明がなされています。セキュリティマネジメントの実施にあたって有用なコントロールを選択することができます。

4.1.2 GMITS におけるリスク分析

GMITS において、特に注目すべきはリスク分析に関する記述です。本書では、第 3 章で詳細リスク分析を紹介しました。GMITS では詳細リスク分析の他に、ベースラインアプローチ、非公式アプローチ、複合アプローチの 3 つの分析手法が紹介されています。個々の分析手法の詳細な解説は、ここでは省略しますが、ベースラインアプローチとは、あらかじめ一定のセキュリティレベルを設定し、それを実現するために必要なコントロールの組合せを決定し、全ての情報資産に対して一様にこのコントロールの組合せを適用する方法です。非公式アプローチとは、分析対象に精通した個人の経験的な判断によって、コントロールを決定する方法です。複合アプローチとは、重要な資産に対しては詳細リスク分析を適用し、それ以外の資産に対してはベースラインアプローチを適用する方法です。複合アプローチでは、まずはじめにハイレベルリスク分析と呼ばれる分析対象全体を俯瞰し詳細リスク分析を適用する資産とベースラインアプローチを適用する資産を選別する分析を行います。

詳細リスク分析は、分析精度が高い反面、膨大なコストがかかる分析手法であることは既に述べた通りです。そこで、実際にリスク分析を実施する場合には、複合アプローチを採用することが、現実的な解決策になります。

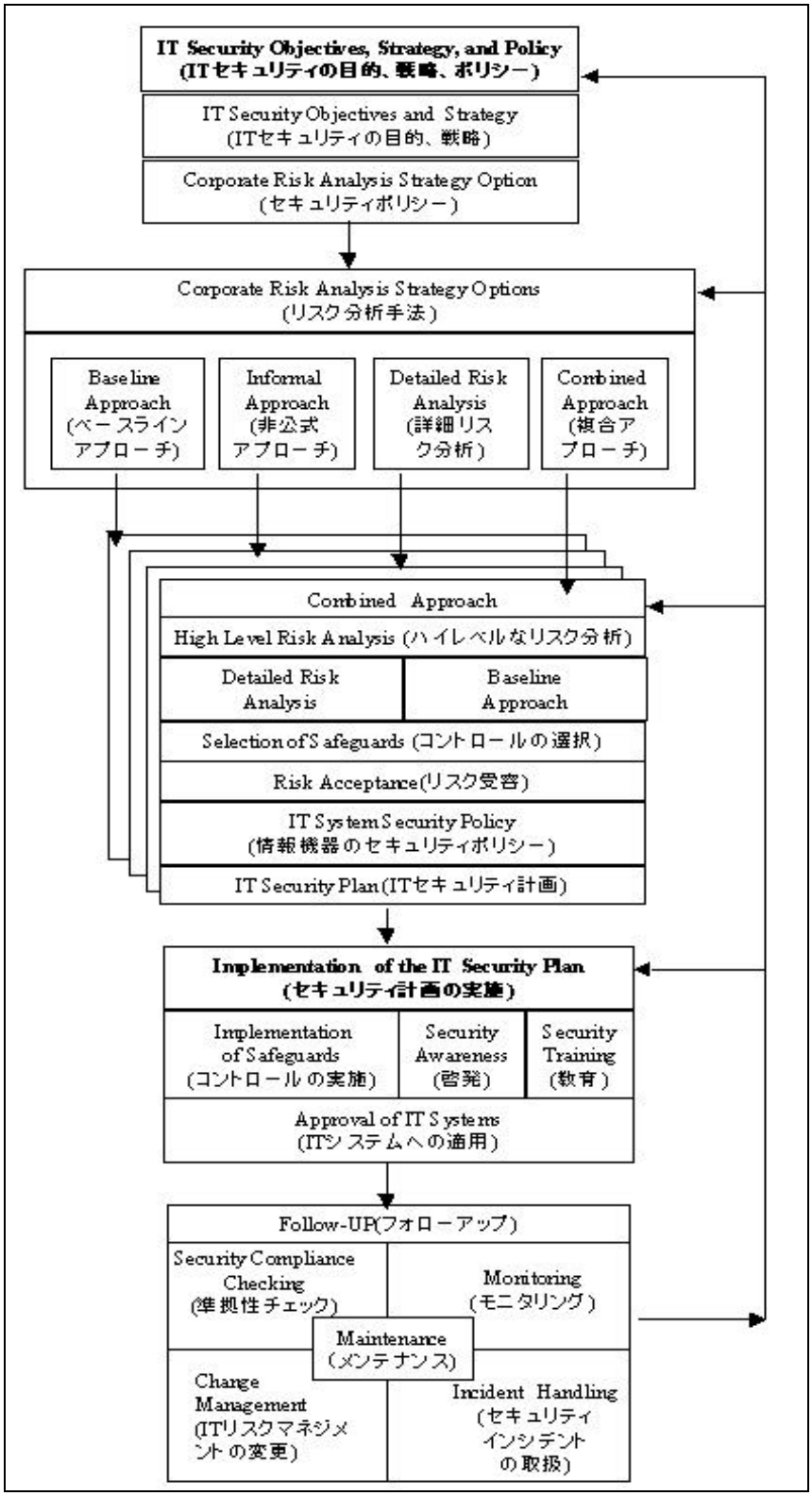

図 4-1　GMITS における IT リスクマネジメントの流れ[40]

[40] ISO/IEC TR 13335 Part1 より。

4.2 BS 7799

4.2.1 BS 7799 の構成

BS 7799 は、1995 年に英国規格協会によって情報リスクマネジメントにおける産業界のベストプラクティスが取りまとめられたことが始まりです。その後、何回か改訂が行われ、2001 年 1 月現在では、2 部構成となっています。BS 7799 では、非電子媒体による情報もその対象に含まれ、GMITS で対象としている IT セキュリティよりも広義の情報セキュリティの立場がとられています。

第 1 部　情報セキュリティマネジメント実施規準

BS 7799 の第 1 部では、情報リスクマネジメントで実施されるコントロールのベストプラクティスが収録されています。収録されているコントロールは、情報システムが工業及び商業分野で使用さるあらゆる場面が想定されており、また組織の規模や営利団体、非営利団体を問わずに利用できるように考慮されています。そのため、第 1 部で取り扱われている全てのコントロールが、あらゆる状況に関連しているわけではないことには注意が必要です。

第 2 部　情報セキュリティマネジメントシステム仕様

BS 7799 の第 2 部には、ISMS（Information Security Management System：情報セキュリティマネジメントシステム）に関する要求事項が記述されています。ISMS とは、第 1 部に収録されたコントロールを実施するための管理的なフレームワークのことを指します。具体的には、ポリシーを定めて、リスク分析に基づき実際のコントロールを決定するシステムを確立することが求められており、これは GMITS で提供されている情報セキュリティの管理モデルとも一致しています。

BS 7799 は、第 1 部が 2000 年 11 月に ISO/IEC 17799 として ISO 化されました。また、日本国内では、平成 13 年 3 月 31 日をもって「情報処理サービス業情報システム安全対策」に基づく事業所認定基準を廃止し、2001 年度中に BS7799 を踏まえた新たな認証制度の創設が予定されています。

4.2.2 情報システム部門責任者の BS7799 の利用

BS 7799 の第 1 部はしばしばセキュリティポリシーを策定する際のガイドラインとして利用されますが、冒頭から順番に目を通していくことはあまり効率的ではありません。これは、第 1 部で取り扱われている各種のコントロール項目には、その並び方に規則性がなく、また様々なベストプラクティスが例として列挙されているため、採用する必要のないコントロールが多数存在するからです。BS7799 を元にセキュリティポリシーを策定する場合は、以下の利用方法が効果的であると考えられます。

① BS7799 全体に目を通し自社に関係のあるコントロールをチェックする。
② 各種コントロール項目に対する具体的なあるべき姿を考える。
③ 各項目のベストプラクティスを例文として参照し、記載レベルを合わせるための視点として利用する。
④ 自社のセキュリティポリシーの各項目が BS7799 のどの項目に該当するかの関連付けを行い、抜け漏れや重複をチェックすることでセキュリティポリシーの網羅性を確保する。

また、独自環境に対する特段の考慮はされていないため、あくまでも手引書・勧告書としての利用が前提であり、利用にあたっては各社の置かれた環境をよく考慮しておくことが求められます。

4.3 情報セキュリティに関する評価認証制度

4.3.1 ISO/IEC 15408 情報技術セキュリティ評価基準[41]

ISO/IEC 15408 は、情報技術に関連した製品およびシステムが情報セキュリティの観点から適切に設計、実装されているかどうかを評価するための評価基準です。現在、ISO/IEC 15408 に基づく評価認証制度が各国で整備されつつあります。日本でも情報処理振興事業協会セキュリティセンターが中心となって、評価認証制度の設立に向けて活動を行っています。

ISO/IEC 15408 は、製品やシステムが備えるべきセキュリティ機能についてまとめられた機能要件集と、製品やシステムが機能要件に定められた機能についてどこまで保証するかについてまとめられた保証要件集から構成されています。そして、保証要件への充足度合いを表す尺度として、7 段階の EAL（Evaluation Assurance Level：評価保証レベル）を設定しています。

ISO/IEC 15408 の規格が適用されるのは、情報技術を用いた製品やシステムであり、個々の組織の情報セキュリティマネジメント体制は評価対象になりません。そのため、情報システム管理部門ではなく、システム開発部門での利用が想定されます。

4.3.2 プライバシーマーク[42]

プライバシーマークは、事業者の個人情報の取扱いに関する評価認証制度で、財団法人日本情報処理開発協会（JIPDEC）によって運営されています。認定事業者は「プライバシーマーク」と呼ばれるロゴマークを使用することができます。

図 4-2　2001 年 1 月現在のプライバシーマーク

41 http://www.ipa.go.jp/security/ccj/download.htm
「ISO15408 情報セキュリティ入門」内山政人（TDU）2000 年

42 http://www.jisa.or.jp/index-j.html

認定にあたっては、JISQ15001「個人情報保護に関する準拠性・プログラムの要求事項」に適合した準拠性・プログラムを策定、実践し、その遵守状況に関する審査を受ける必要があります。2001 年 2 月現在で 196 事業者がプライバシーマークの認定を受けています。

4.3.3 WebTrust[43]

WebTrust は、米国の公認会計士協会が運営する、会計監査のフレームワークに沿った Web サイトの安全性保証サービスです。WebTrust では、業務開示、取引完全性、情報保護の 3 つの観点から総合的に Web サイトの安全性を保証します。

業務開示の観点からは、Web サイトを運営する事業者がサイト上で提供しているサービスに関する情報を適切に開示しているかどうかを確認します。取引完全性の観点からは、サービスで合意された取引が、合意内容通りに取り進められているかどうかを確認します。情報保護の観点からは、サービスで知り得た個人情報が適切に取り扱われているかどうかを確認します。

WebTrust の認定を受けた事業者は、WebTrust マークをホームページへ掲示することが許されます。WebTrust は特に Web サイトで BtoC ビジネスを展開している事業者が、消費者に安心感を付与するために効果的です。

図 4-3　2001 年 1 月現在の WebTrust 認証シール

[43] http://www.cpawebtrust.org/

4.4 国際的ガイドラインの利用方法

第 4 章では、情報セキュリティに関する様々な国際的ガイドラインを紹介しました。ここで、これらのガイドラインは汎用的に利用されるように作成されています。そのため、ガイドラインで示されている全ての項目を遵守しようとすると、実態にそぐわない項目に対しても無理やり適合することを強いられ、結果として業務に支障を来してしまうことがあります。ただ闇雲にガイドラインへの準拠を謳うのではなく、自社のビジネスを取り巻く状況を冷静に判断した上で、準拠する必要のあるガイドラインと準拠の度合いを決定する必要があります。また、これらのガイドラインにはセキュリティレベルの全体的な底上げを目的として作成されているものと、セキュリティレベルの更なる高め誘導を目的として作成されているものがあります。国際的ガイドラインへの準拠を検討する場合には、この両者を使い分ける必要があります。

そして、このような理由から、国際的なガイドラインに基づく評価認証制度については、各企業がそれぞれ必要性を検討した上で、自ら挙手する姿勢が本来は望まれます。一時期 ISO9000・14000 シリーズの取得が一種のブームのようになりました。その結果、国際標準規格だから守らねばならないといった短絡的な発想に基づいた社内規定が多数作成され、ISO を取得はしたものの業務手順書を遵守しようとすると、膨大な量の資料保管や確認手順が要求されるため遵守が事実上不可能となり、更新審査の前後 1 週間だけ集中して書類を整理している、という企業が多数見受けられます。このような形で国際標準規格を導入したとしても、安定的な業務の標準化にはつながりません。

国際標準規格を採用する場合には、自社の採用目的を明確にし、目的達成のために必要なツールとして規格を使いこなすという視点が大切です。

5 結び[44]

IT ガバナンスに基づく情報リスクマネジメントの重要性、そして情報リスクマネジメントを実践するために必要となる膨大なコストについて理解を深めることができたでしょうか。

「なぜ情報リスクマネジメントが必要なのか」に対する答えが見えてきたことと思います。しかし、次に待ち構えているのが本文中にも幾度となく登場した、「部門間の壁」と「予算獲得の難しさ」です。多くの情報システム部門の責任者が、セキュリティ対策予算の獲得に失敗し、例え成功したとしてもセキュリティ対策の実施段階で、他部門からの協力を得られずに中途半端なコントロール実施を余儀なくされています。中途半端な対応は、セキュリティ対策の重要性に対する組織の理解を削ぎ、社員からセキュリティ対策に積極的に取り組もうというモチベーションを奪います。

次頁から、IT リスクマネジメントの現状チェックリストを掲載します。自社にかけている視点、遅れている対策を簡便に確認することができます。章節の列に記載された番号は、関連する本書の章節の番号です。予算獲得、部門間調整にあたって、説明が求められた際などに利用する索引としても利用可能です。

---

44 「IT マネジメント」半田　純一（東洋経済新報社）2000 年
「ネットワークリスク診断チェックリスト」日本損害保険協会（http://www.sonpo.or.jp/）

	確認項目	YES/NO	章節
全社戦略と情報システム投資戦略の関連	全社 IT 投資方針、計画といったものが作られている。	YES/NO	2-1
	全社の IT 投資方針と経営計画の間に関連性がある。	YES/NO	2-1
	全社の IT 投資方針、計画を議論する際には、IT 組織のみで議論せず、業務部門の実状や意見を積極的に取り入れている。そのため、現場への説明が方針決定後になることはない。	YES/NO	2-1 3-4-1
	経営戦略を議論するとき、情報システム部門責任者が同席する。	YES/NO	2
	経営戦略の策定は経営企画部門と情報システム部門が協力して行い、結果だけが情報システム部門に説明されるようなことはない。	YES/NO	2
役員レベルでの情報システム・情報セキュリティへの取組み	役員の中に、システム構築作業に実際に関わりプログラミング・機器選定などに関わったことのある人間がおり、システム開発・投資で発生しがちな問題や効果を身をもって理解している。	YES/NO	2 3-4-1
	システム関連投資プロジェクトの最終決裁権を持つ役員会は、予算と金額だけではなく、投資によってもたらされる効果を的確に理解した上でプロジェクトの採否決議を行うことができる。また、事実行っている。	YES/NO	2-3
	役員会・情報システム部門責任者は、自社の情報システム部門の能力が同業他社と比較してどの位置にベンチマークされるのか十分理解している。	YES/NO	2-3 3-1
	役員会・情報システム部門責任者は、自社の従業員の情報リテラシーが同業他社と比較してどの位置にベンチマークされるのか十分理解している。	YES/NO	2-3 3-1
情報システムの投資効率に関する意識の高さ	システム関連投資プロジェクトが大幅に予算や期間をオーバーしたり、大幅に予定を下回るようなことはない。	YES/NO	2-3 3-5 3-7
	システム関連プロジェクトは一回スタートしても、定期的に見直し作業を行い、予算・期間・目的・効果などに疑問があれば中断されることもある。	YES/NO	3-5
	今年度のシステム関連投資予算と実際のシステム関連投資額を役員全員と情報システム部門責任者が即答できる。	YES/NO	2-3-7
	情報システム部門には、人数的・スキル的に十分な人材がいて運用管理とは別に新規開発・改善活動に携わることができる余裕がある。	YES/NO	3-7
	情報システム部門には、セキュリティ問題に専門に従事する人材を用意しており、セキュリティホールが発見された場合には即時対応が可能である。	YES/NO	3-6

	確認項目	YES/NO	章節
社内情報伝達の透明度	自社で今後、IT を利用して積極的に促進すべきビジネス領域が複数思い当たる。また、そのビジネスの所管部署がどこであるか理解している。	YES/NO	2-2
	システム関連コストの削減・効率性向上にあたっては、全体で何%といった大まかな計画ではなく、細かく業務やシステム、プロセス別に実現可能な目標を定めて実行している。	YES/NO	2-3
	社内標準のプラットフォーム、アーキテクチャが存在しており、それから外れた開発やシステム導入が必要な場合は情報システム部門・業務部門を横断した情報交換が行われ、役員会レベルの決裁を要する。	YES/NO	3-4-1
	経営企画・人事・総務などのマネジメント部門の従業員に対して、十分な情報リテラシー教育が行われている。	YES/NO	3-4-3
	情報システム部門の従業員に対して、十分なマーケティング・経営戦略論などのビジネス教育が行われている。	YES/NO	3-4-3
情報システム部門と他部門の関係性	情報セキュリティにかかわる組織が明確になっている。	YES/NO	3-4-1
	情報セキュリティを統括する担当役員や最終意思決定機関が文書化されており、従業員に周知してある。	YES/NO	3-2 3-4-1
	セキュリティポリシーが文書化されており、従業員に周知してある。	YES/NO	3
	情報セキュリティ管理者の育成プログラムがある。	YES/NO	3-2
	全従業員に対して情報セキュリティ教育が行われている。	YES/NO	3-4-3
	新入教育の中に情報セキュリティ教育が含まれている。	YES/NO	3-4-3
情報リスクマネジメントレベルの把握	定期的にシステム監査を実施している。	YES/NO	3-5
	情報システム監査を実施し、監査結果を適切に反映している。	YES/NO	3-2
	不測事態（災害、大規模障害等）の対策を講じている。	YES/NO	3-5-1
	アウトソーシングを行う場合、委託先のセキュリティ対策状況を評価している。	YES/NO	2-2
	ハードウェアの購入および資産管理台帳に基づいた資産管理が適切に行われている。	YES/NO	3-2
	コンピュータ機器の導入に関して、選定・取得・設置・接続・変更に関する承認手続が定められている。	YES/NO	3-2
	ネットワーク構成図は最新の状態で作成されている。	YES/NO	3-2
	ソフトウェアの購入および資産管理は適切に行われている。	YES/NO	3-2
	ソフトウェアの資産管理台帳に基づいて、すべての PC、サーバにインストールされているソフトウェア構成を把握している。	YES/NO	3-2
	業務以外の利用を制限するルールがある。	YES/NO	3-2
	ホームページのコンテンツセキュリティ対策を行っている。	YES/NO	3-2
	ワクチンソフトウェアは、すべての PC、サーバにインストールされ、メモリに常駐（常駐監視）させている。	YES/NO	3-4-4
	定期的に侵入テストを実施している。	YES/NO	3-5-1

情報セキュリティ部門責任者のための
情報セキュリティブックレット

情報処理振興事業協会
セキュリティセンター

〒113-6591　東京都文京区本駒込 2-28-8
文京グリーンコート
センターオフィス 16F
FAX： 03-5978-7518
e-mail: isec-info@ipa.go.jp