エンタープライズ・セキュリティー・マネジメント・アーキテクチャー

これからの時代にふさわしい企業のセキュリティー・マネジメントの骨格となる、新たなマネジメント・アーキテクチャーを定義するには、これまでのセキュリティー・マネジメントが持つ課題を整理する必要があります。これによって、今後を担う企業にとっての有効な手法が明確になります。企業のセキュリティー・マネジメントの確立は、これまでのようにセキュリティーに関する課題のみに専念するのではなく、企業改革のプログラムとして位置付けることが重要です。また、新たなマネジメント・アーキテクチャーを完成させるには、ラインとスタッフの基本的な関係を整理したうえで、CSO（Chief Security Officer：最高セキュリティー責任者）を中心とした組織体系を定め、「コントロール」と「マネジメント」の実施責任を明確にする必要があります。本論文では、従来のセキュリティー・マネジメントの持つ課題の整理と組織体系の明確化といった作業を通して、その概念をITセキュリティーから情報セキュリティーへと広げ、企業が取り組むべきあらゆるセキュリティーの課題に適用できる可能性を示します。そして、このアーキテクチャーが、マネジメントの課題の解決にいかに役立ち、ひいてはビジネス・プロセス・アウトソースの一環として、セキュリティー・マネジメントのアウトソースの枠組みを定めるためにも価値が高いことを示します。

アイ・ビー・エム ビジネスコンサルティング サービス株式会社
チーフ・セキュリティー・オフィサー（CSO）、パートナー、
IBMディスティングイッシュト・エンジニア、IBMアカデミー会員
Chief Security Officer, Partner,
IBM Business Consulting Services KK
IBM Distinguished Engineer, Member of IBM Academy of Technology

大木 栄二郎 **Eijiroh Ohki**

［プロフィール］
1970年、日本アイ・ビー・エム入社。大規模ネットワーク管理システム開発や、国際VANの推進などネットワーク・サービスの拡充担当を経てコンサルティング事業部へ移籍。ネットワークとセキュリティーを中心としたコンサルティングを担当。日本アイ・ビー・エムにおけるセキュリティー・コンサルティングの分野を確立し、数多くの企業のセキュリティー診断やポリシー策定などの経験を持つ。経済産業省や総務省などの情報セキュリティー関連委員会の委員を歴任。日本セキュリティ・マネジメント学会理事、NRA幹事、メール・マガジン『啓・警・契』編集長として、情報セキュリティーの啓発普及にも活躍している。著書『経営戦略としての情報セキュリティ』（工業調査会）など。

Enterprise Security Management Architecture

We need to gain a firm grasp of the issues faced hitherto by security management in order to define the new management architecture that will serve as the framework of corporate security management suitable in the age to come. This will make it possible to clarify the methods likely to prove effective for the companies that will be playing important roles in the future. Establishment of corporate security management should involve not only topics concerned with security as it has done in the past; it is important that it should be thought of as part of a program of corporate reform. Moreover, in order to put together a new type of management architecture, it is going to be essential to determine an organizational structure centering on a CSO (Chief Security Officer) after having clarified the basic relationships applying among lines and staff, and further to bring into clear focus the nature of the duties to be executed by ÅgcontrolÅh and Ågmanagement.Åh In this paper I attempt to clarify the issues dealt with in the past by security management and to throw light on organizational structures in order to expand this concept from IT security to information security and to show the possibilities for application to all kinds of security issues faced by companies. I show how this architecture can be of use in the solution of management issues, and I then go on to show that it may even be a valuable way of determining the frameworks of security management outsourcing within the context of business process outsourcing.

1. はじめに

IBMの提唱するe-ビジネスの本格化に伴い、「IT革命を!」や「電子政府を!」といったスローガンの下に、世の中全体が従来の工業化社会的な価値観から、情報に相対的な価値を置く情報化社会への転換が動き始めたといえるでしょう。

最近は、ブロードバンド・ネットワークの急速な普及に伴って、パーベイシブあるいはユビキタス・ネットワーク時代というのも現実味を帯びてきて、企業の経営環境が大きく変わろうとしています。

一方では、インターネットを中心に、情報セキュリティーにまつわる事件や事故の類が次々と明らかになり、企業や政府の情報管理が世の中から不審な目で見られるような事態も多発しています。また、その延長線上には、企業の倫理観や経営者のリスク・マネジメント能力が問われる事態も起きています。このような背景の中で、企業はあらゆる面で新たなマネジメントの確立が求められています。

本論文では、こうしたもののうち、「セキュリティー・マネジメント」について論述します。

2. セキュリティー・マネジメントの課題

セキュリティー・マネジメントには、大きく分けて次に挙げる四つの課題があります。

ESMA(Enterprise Security Management Architecture)は、これらを解決するための道具として使えるものでなければなりません。

(1)時代の変化に応じた意識改革あるいは企業文化の変革の側面があり、全社員の理解と同意を確認しなければならない。

(2)BS7799など、「ベスト・プラクティス」と呼ばれる国際的な標準化が進んでいる。しかし、その対象は脆弱(ぜいじゃく)性の補強などに要求されるコントロール策が中心で、各論での現場の抵抗なども大きく、実現への道は必ずしも平坦ではない。要求されるコントロール策を具体的に推進していくマネジメント部分は、必ずしもベスト・プラクティスの標準規格では示されてはいない。

(3)急速な技術の変化、セキュリティー・フレームワーク、リスク分析手法、領域別に要求されるコントロール策、安全性検証手法など、特殊なスキルや経験を必要とする活動が各所に部分的に含まれており、人材不足ということもあって、必要なスキルド・リソースの確保やその分散配置などが難しい。

(4)実施責任、管理責任の所在が不明確になりやすくあいまい。このため、コントロール施策の実施が進まない。

セキュリティー・マネジメントの考え方は、情報セキュリティーやITセキュリティーを中心として発展してきました。最近では、各種の国際標準も制定され始めています。しかし、残念ながら、セキュリティー・マネジメントの明確な定義は、まだ定着していないのが実情です。

国際的には、ISO-17799やISO-13335などが情報セキュリティー・マネジメントの体系について定義していますが、情報を取り扱う際に求められるコントロール(統制)を主体として記述されており、企業活動全般のリスクまでには広げてはいません。セキュリティー・マネジメントを冠した国際的な学会(日本セキュリティ・マネジメント学会)がありますが、セキュリティー・マネジメントそのものの定義は明らかにはしていません。

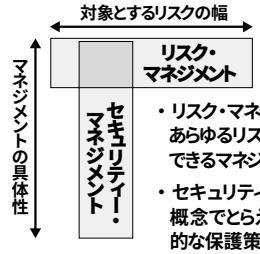
本論文では、セキュリティー・マネジメントを、

「情報を中心として発展してきたセキュリティーの考え方を現代の企業を取り巻くさまざまなリスクに適用して、企業の各種資源や活動の安全を確保するためのマネジメント体系」

と定義し、当面は情報セキュリティーに適用し、そのほかの経営資源のセキュリティー・マネジメントにも適用可能であることを示しておきます。

3. セキュリティー・マネジメントとリスク・マネジメント

セキュリティー・マネジメントとリスク・マネジメントは、最近で



・リスク・マネジメントは、経営に影響を与えるあらゆるリスクを対象として、包括的に対処できるマネジメント・システムを指向する。

・セキュリティー・マネジメントは、“ 安全 ”の概念でとらえるべきリスクを対象とし、具体的な保護策の有効性を指向する。

	歴史的背景と世の中の受け止め方	これからの戦略と整合性
リスク・マネジメント	・危険分散 ・他責事項への保険 ・損失の回避 ・財務的発想	△
セキュリティー・マネジメント	・安全対策 ・自責事項の徹底 ・信頼醸成 ・具体的施策	◎

図1. セキュリティー・マネジメントとリスク・マネジメントの違い

はよく耳にする言葉です。両者はともに、企業活動における各種のリスクに対して、企業が取るべき対処法の検討や実施、その評価などを包含します。一見、同様の分野に対する同種のマネジメントととらえられがちですが、その本質的な見方はかなり異なります。図1に、セキュリティー・マネジメントとリスク・マネジメントの違いを示します。

まず、セキュリティーは、「物事の安全を、どのように確保するか」という安全側から見ているのに対し、リスクは、「危険がどのように発生し襲ってくるか」を危険側からとらえています。この意味で、セキュリティーとリスクは一つの事象の表と裏の関係にあると見ることもできます。

リスク・マネジメントは、本質的にコントロール不可能な不確実性に対する危険分散がそもそもの由来であるのに対し、セキュリティー・マネジメントは、自分で取れる安全対策をどう構築するかが主眼です。最近の企業のリスク・マネジメントのとらえ方は、企業活動に影響のあるすべてのリスクを対象とし、包括的に対処できるマネジメント・システムを指向しているのに対し、セキュリティー・マネジメントは、安全の概念でとらえられる範囲のリスクを対象とし、具体的な保護策の有効性を指向します。その意味で、リスク・マネジメントはより包括的であり、セキュリティー・マネジメントはより具体的であるともいえます。

つまり、リスク・マネジメントは幅広いリスクを対象としますが、本来は不確実な危険分散を意図したものであり、他責事項に対する保険的色彩が強く、損失の回避などの財務的発想に基づいています。一方、セキュリティー・マネジメントが対象とするリスクは、安全という概念でとらえられる範囲ですが、具体的な安全対策を指向し、自責事項の徹底に重点が置かれ、信頼醸成や具体的施策に結び付く特徴があります。

このように整理すると、社会全体を取り巻く情報化社会的な価値観への大きな変革のうねりの中で、企業はさまざまなリスクへの対応が求められる中、セキュリティーの概念を中心に据えて、新たなマネジメントを確立することが大きな効果をもたらす可能性が高いといえるでしょう。

また、ITセキュリティーの分野で検討されてきたリスクの構造分析（例えば、ISO/IEC TR-13335で示されているリスク要因）の結果をより一般的にすることで、より広く役員や社員といった関連する人の安全や物資、施設、設備、建物など、そのほかの資源のセキュリティー確保にも適用可能であると考えられま

［脅威］が	［脆弱性］をついて	［事象］を引き起こす（想定被害）
• 経営環境の脅威 – 自然現象 – 国家／法律／税 – 市場／競争 • 経営資源に潜む脅威 – 人 – もの – かね – 情報	• ビジネス・プロセス • 組織・人 • アプリケーション • ITインフラストラクチャー	• 経営 • 情報 • 工場・設備 • 人材 • 信用 • 反社会的行為 • 自然災害

図2. リスクの構造

脆弱性の4面での整理と担当すべき組織の基本的配置

ビジネス・プロセス	組織	ソリューション（アプリケーション）	インフラストラクチャー
【重要プロセスの欠落】 ・QAプロセスの欠如 ・監査欠如 法務部 【プロセスの機能不全】 ・人員不足、資源不足、予算不足 ・非効率的プロセス ・出力品質低下 ・処理バイパス ・処理漏れ ・誤処理 ・誤出力 【プロセスの不整合】 ・旧態依然の処理 ・前後のプロセスと合わない 【検証不足】 ・入力チェックなし ・チェックなし承認 ・けん制機能不備 事業部 【プロセスの品質基準なし】 ・品質フィードバックなし	【組織】 ・企業文化・風土 ・ミッション不明確、漏れ ・戦略と組織の整合性 ・ビジョン ・リーダーシップ 経営企画 ・センシティビティー ・権限不明確／不備 ・権限の不十分な分離 【人】 ・知識／スキル不足 ・柔軟性欠如 ・目的意識／モラル欠如 ・教育・訓練不足 ・経験不足 ・理解不足 ・準備不足 人事部 ・無知無能 ・ポリシーへの順守欠如 ・無管理下での作業（外部または清掃職員） ・不十分な雇用手順 ・人員の不在または不足	【機密性】 ・データ暗号不備 ・ファイル保護不備 ・暗号鍵管理不備 【完全性】 ・データ完全性確認機能不備 ・データの完全性保証機能不備 ・統制確認機能不備 ・耐監査性機能不備 【可用性】 ・システムとデータ回復管理 ・キャパシティー管理 ・データ・バックアップ管理 【識別認証】 ・ユーザー認証不備 ・弱いパスワード ・認証ファイル保護欠如 【アクセス制御】 ・権限付与管理 ・登録手順 IT部 【否認防止】 ・否認防止機能不備	【建物・設備】 ・不安定な地理的な場所 ・物理設備 ・建物構造 ・警備 ・防火設備 総務部 ・メンテナンス ・整備不良 ・設計不備 ・工事ミス ・視覚的なIDカード着用違反 【システム・ネットワーク】 ・高信頼設計不備 ・ネットワーク・アクセス管理 ・コミュニケーション暗号管理 ・ネットワーク認証 ・データ通信の完全性保証 ・DNS配置と保護管理 ・ネットワーク・ルーティング管理 ・DoS攻撃への管理 ・無防備のコミュニケーション・ライン ・反監視管理 ・侵入者検出 IT部 ・セキュリティー事故報告の仕組み ・事故対応訓練 ・アクセス・ログ管理と監査

図3. 脆弱性と担当組織の関係

す。すなわち、企業の内外に存在する脅威が、企業のビジネスやITの中に潜む脆弱性を突いて、経営に影響を与えると考えるのです。

企業の経営リスクについては、会計監査の観点から、あるいは損害保険の観点から、従来の事故例が多角的に分析されています。これらには、ケース・スタディー的に分析し、経営に影響を与えた事象で分類されているケースが多くあります。

こうしたケースを実際にこの構造に当てはめてみると、それらのほとんどが、このリスク構造に基づいて分析でき、企業が取るべき対策が、この構造から明確に指摘できることが分かります（図2）。

図3は、実際のこうしたケースの分析で現れた企業の脆弱性を、ビジネス・プロセス、組織、ソリューション、インフラストラクチャーの四つの面に分類して整理した例を示しています。

さらに、このリスク構造の考え方に基づくと、企業がこうしたリスクに対応するマネジメントを確立する上での部門間の基本的な役割分担を示すこともできます。セキュリティー・マネジメント自体が、自責事項への対策を取ることに中心があるとしたことからもある程度自明ですが、その基本は脆弱性に注目して、セキュリティー対策を検討する責任部門を定めるという考え方です。企業のプロセスや仕組みをビジネスとITの両面から大きく四つの面で整理し、その要素ごとに脆弱性に対応すべき組織を考えることで責任部署を定めるのです。

4. ESMA (Enterprise Security Management Architecture)

4.1. コントロールとマネジメントの分離

日本語でいう「セキュリティー管理」には、英語でば“ Security Control ”と“ Security Management ”の2種類の意味が含まれています。いずれも、日本語では「セキュリティー管理」と訳されることが少なくありませんが、それぞれの本質はかなり異なります。

「コントロール」は、「管理」というよりも「統制」という言葉の方が本質に近く、セキュリティーを守るための施策を講じると決めたらその通りに現場が動き、所要の条件を満たした活動ができることを指します。一方、「マネジメント」は、決めた通りになかなか物事が運ばない場合でも、何とかやりくりをして、計画に沿って目標を達成する活動を指します。

この「コントロール」と「マネジメント」の両方の差をはっきりと意識して、両者が有機的に絡み合って初めて、“ Security Management ”が機能することになります。ここが、ESMAの根幹です。

「コントロール」を縦軸に、「マネジメント」を横軸に、それぞれ

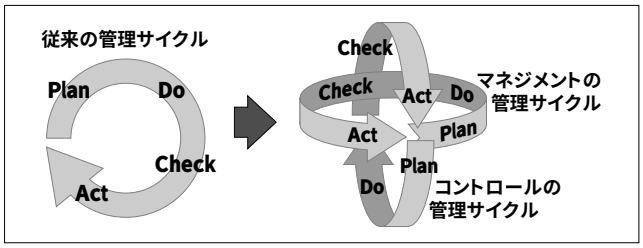


図4. コントロールとマネジメントの分解

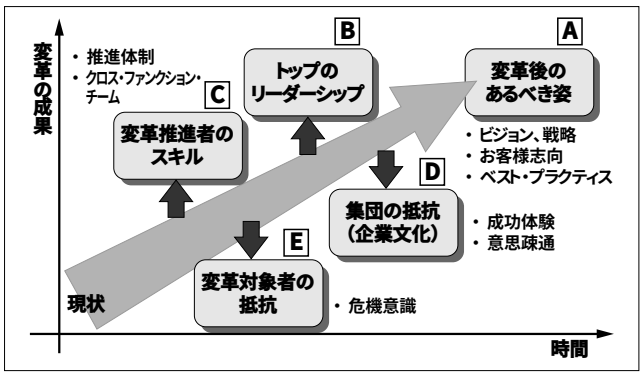


図5. チェンジ・マネジメントの成功要因

を有機的に関連した体系として定義し、それぞれの実施責任を組織的に明確化することにより、大きな時代の節目におけるマネジメント・システムの改革が可能となります（図4）。

4.2. 変革のマネジメント

セキュリティー・マネジメントの確立を大きな時代背景から分析すると、工業化社会的価値観から情報化社会的価値観への転換過程にあると考えられます。単にセキュリティー・マネジメントが経営の大きな課題であるだけでなく、同時にビジネス・モデルやビジネス・プロセスも大きく変革しなければならない状況にあるはずです。セキュリティー・マネジメントの確立は、同時に企業の文化や風土の新しい時代に向けての変革や、それに伴う社員全員の意識改革的な色彩も帯びることになります。

従って、全社セキュリティー・マネジメントの確立と向上には、チェンジ・マネジメントの五つの要因が成功のカギを握ります（図5）。

（A）改革後の“ あるべき姿 ”

企業改革後の“ あるべき姿 ”を、セキュリティー・マネジメントだけで描いて変革を方向付けるのは少し難しいかもしれません。ただし、企業戦略としての変革の姿があることを前提にすると、セキュリティー・マネジメントの“ あるべき姿 ”をセキュリティー・ポリシーに描くことで、企業全体の変革プログラムの中に明確に位置付けられます。

（B）トップのリーダーシップ

CSO（Chief Security Officer：最高セキュリティー責任者）あるいは情報セキュリティーのみを担当すると明確化する場合は、

CISO（Chief Information Security Officer：最高情報セキュリティー責任者）のミッションを明確に定め、シニア・マネジメントをアサインし、的確なスタッフを集めることで、リーダーシップを確立することができます。

（C）変革推進者のスキル

セキュリティー・マネジメントのスキルは、残念ながら一般的にはなっておらず、最も重大な阻害要因として浮かび上がります。CSOスタッフの組織にスキルのある人間を集中配置し、そこにスキルの必要な活動も集中させることが、成功のカギを握ります。

（D）集団の抵抗を少なくする（企業文化）

セキュリティー・マネジメントを中心に企業分化を先導するのにはかなりの無理があります。企業戦略として、情報化社会への転換をどう位置付けるかが中心であるべきであり、その補助的条件としての情報の価値の増大に見合うセキュリティー意識の改革などにつなぐことで、当然全社員がその方向に進むべきだという雰囲気づくりが必要です。

（E）変革対象者の抵抗を少なくする

マネジメント体系の定義から出てくる管理プログラムやキャンペーンにより、変革対象者の抵抗を跳ね返して、実効を上げていく工夫が必要です。変革対象者の抵抗を乗り越える最大の要因は、情報の開示です。どの部門が抵抗しているのか、およびどの部門は変革が進んでいるのかを客観的なデータとして開示し、冷静な判断で対応できるようなプログラムが必要です。

表1. ISO-17799のコントロールの体系

大分類／中分類		中項目数	小項目数
3	セキュリティー・ポリシー	1	2
	3.1情報セキュリティー・ポリシー		2
4	セキュリティー組織	3	10
	4.1 情報セキュリティー基盤		7
	4.2 第三者アクセスに対するセキュリティー		2
	4.3 アウトソーシング		1
5	資産の分類および管理	2	3
	5.1 資産に対する責任		1
	5.2 情報の分類		2
6	人的セキュリティー	3	10
	6.1 業務定義および配置におけるセキュリティー		4
	6.2 ユーザーの訓練		1
	6.3 セキュリティー事故および誤動作への対処		5
7	物理的および環境的セキュリティー	3	13
	7.1 セキュリティー領域		5
	7.2 装置のセキュリティー		6
	7.3 一般コントロール策		2
8	通信および運用管理	7	24
	8.1 運用手順および責任		6
	8.2 システム計画および受け入れ		2
	8.3 悪意があるソフトウェアに対する保護		1
	8.4 維持管理		3
	8.5 ネットワーク管理		1
	8.6 媒体の取り扱いとセキュリティー		4
	8.7 情報およびソフトウェアの交換		7
9	アクセス・コントロール	8	31
	9.1 アクセス・コントロールに対するビジネス要件		1
	9.2 ユーザー・アクセス管理		4
	9.3 ユーザー責任		2
	9.4 ネットワーク・アクセス制御		9
	9.5 オペレーティング・システム・アクセス制御		8
	9.6 アプリケーション・アクセス制御		2
	9.7 システム・アクセスと使用のモニタリング		3
	9.8 モバイル・コンピューティングとテレワーキング		2
10	システム開発と保守	5	18
	10.1 システムのセキュリティー要件		1
	10.2 アプリケーション・システムのセキュリティー		4
	10.3 暗号の管理		5
	10.4 システム・ファイルのセキュリティー		3
	10.5 開発とサポート・プロセスのセキュリティー		5
11	ビジネス継続管理	1	5
	11.1 ビジネス継続管理の観点		5
12	規定の順守	3	11
	12.1 法的な要求への順守		7
	12.2 セキュリティー・ポリシーと技術的準拠のレビュー		2
	12.3 システム監査上の考慮点		2
	合計	36	127

※大分類番号はISO-17799の章番号をそのまま採用したので、3から12の10分類となっている。

4.3. コントロール体系

これまで、セキュリティー・マネジメントの標準化の努力のほとんどは、このコントロールの定義に割かれています。すなわち、どのような手順で何をすればセキュリティーを確保するための統制が取れるのかの設計に、多くの努力が割かれているといえます。それらの成果として示されているコントロールの候補策から、その企業にとってのあるべきコントロールを体系的に整理して、その実装を管理サイクルに沿って示すのがコントロール体系です。

現在、この分野の国際規格として活発に引用されている“ ISO/IEC 17799 Information Security Management ”は、1995年に出た英国規格のBS-7799から発展してきましたが、その多くの努力は、有効なセキュリティー・コントロールの定義に焦点を当ててきたといえます。その結果、ISO/IEC19977には、10個の管理領域に分けて127のコントロールがベスト・プラクティスとして定義されています（表1）。

ほとんどの企業が、セキュリティー・ポリシー策定のベースにこの規格を採用しており、セキュリティー・マネジメントの確立に必要なコントロール候補のリストアップは、一応完成形に達していると見ることができるでしょう。ESMAのコントロール体系には、このISO/IEC 17799

Information Security Managementのコントロール策を、10領域に構造化して採用するのが望ましいでしょう。

情報のセキュリティーを中心にコントロール体系の中身を検討しましたが、これを情報以外のそのほかの経営資源のセキュリティーに拡張するのも、この対応の延長線上で考えられます。既にBS 7799の10領域には、人的セキュリティーや物理環境セキュリティー、さらには法令順守などが組み込まれています。ただし、こうした検討の中心が、「情報のセキュリティーを守るためのもの」という前提付きで限定されているのですが、これを経営資源全般に関して拡張して考えることから取り組むことができます。さらに、そのほかの観点からのコントロールをこの体系に追加することで、段階的にセキュリティー・マネジメントの枠を広げることが可能であり、その際にも、脆弱(ぜいじゃく)性の担当部門がそのコントロール策の検討に中心的な役割が期待されることになります。

コントロール体系の核心は、選定されたコントロールが各組織の中で具体的に埋め込まれて機能するための管理サイクル

表2. コントロールとマネジメントの管理サイクル

	コントロール	マネジメント
Plan	定められたコントロールの導入を計画する	必要なコントロール策と実施基準を定める
Do	コントロールを実施する	コントロール策の実施範囲と責任者を定める
Check	コントロールの実施状況を確認する	コントロール実施の進捗や有効性を評価する
Act	コントロールの実施方法を改善する	コントロール策の内容や基準を改善する

（A）施策実施の責任明確化
- A-1 部門ごと、プロダクトごと、社員ごとなど、必要に応じてコントロール施策の実施責任者を付与し、理解を確認する。
- A-2 同意の確認を求める。

（B）施策の実施を促進
- B-1 実施単位ごとの施策の実施状況や進捗を比較し、遅れている部分の把握と尻たたき。
- B-2 内容の充実度を項目や準拠性などで評価し徹底を図る。

（C）施策の有効性を検証
- C-1 施策が実施されているか。
- C-2 施策が日常業務に反映されているか。
- C-3 施策の実施は効率良く行えているか。

図6. コントロール施策の有用性を管理する考え方

表3. コントロールに対応する重点管理目的（抜粋）

			重点管理の目的
領域－1 セキュリティー・ポリシー			
コントロール施策の有効性を管理する考え方			
A.実施責任の明確化			
	A-1 実施責任付与	3.1	各種のセキュリティー関連の規定類が全社セキュリティー方針に基づき体系化された枠組みに沿って作成され、適切なレベルの承認を経て施行されていることを、規定のオーナーが明確であること、定期的に見直され必要に応じて更新されていることを確認する。
	A-2 同意の確認	3.1	規定のオーナーが、オーナーとしての役割と責任を理解しオーナーとしての職責を果たすことについての同意を確認する
B.施策の実施促進			
	B-1 実施進捗比較		該当しない
	B-2 充実度評価	3.1	セキュリティー関連規定それぞれに必要な項目が記載されているか点検する
		3.1	セキュリティー規定の体系を示し、部門ごとにその規定の整備状況を把握する
C.施策の有効性検証			
	C-1 施策の理解度	3.1	すべての社員が、全社セキュリティー・ポリシーを理解し順守することを確認する
	C-2 充実度評価		該当しない
	C-3 実施効率		該当しない
領域－2 セキュリティー組織			
コントロール施策の有効性を管理する考え方			
A.実施責任の明確化			
	A-1 実施責任付与	4.1	CSO、SMO、セキュリティー・マネジメント会議、セキュリティー専門委員会、セキュリティー専門グループ、タイガー・チームなどの役割と責任、そのための権限などを明確に定義され、関係者から理解されていることを確認する
			情報資産のオーナー、ユーザー、サプライヤーの役割と責任が明確にされ、関係者から理解されていることを確認する
		4.2 4.3	第三者に社内情報資源へのアクセスを許可する場合やアウトソーシングにおいて、その責任者にはリスク評価をすることとその結果を契約事項に反映させる責任があることを明確に認識させる
	A-2 同意の確認		該当しない
B.施策の実施促進			
	B-1 実施進捗比較	4.2 4.3	部門ごとに、第三者に社内情報資源へのアクセスを許可する委託あるいはアウトソーシングなどの契約書類全体の中で、リスク評価とその結果の対応が組み込まれていない契約の存在を把握し、対応を促す
	B-2 充実度評価	4.1	セキュリティー・マネジメント会議、セキュリティー専門委員会、セキュリティー専門グループ、タイガー・チームなどが当初の計画通りに機能していることの検証
C.施策の有効性検証			
	C-1 施策の理解度		該当しない
	C-2 充実度評価		該当しない
	C-3 実施効率		該当しない

にあります（表2）。

4.4. マネジメント体系

コントロール体系を縦軸とすると、マネジメント体系は横軸として、定められた各種コントロール施策を担当組織ごとに確実に実施するための管理を体系化するものです。

企業におけるセキュリティー・マネジメントの確立は、情報化社会に向かっての企業の大きな変革をも意味していますが、これまであまり有効な手だてが打たれなかった難しい部分でもあります。ISO/IEC 17799などの国際規格には、コントロールは詳細に記述されていますが（図6）、マネジメントについての具体的な記述は極めて少なくなります。いかに的確な手段で組織的な努力が払われるかに、この重要な変革の成否がかかっているといっても過言ではありません。

まず、10領域で整理されたコントロール体系の各項目ごとに、あるべきコントロールを選択し、その基準や具体策を定めることがマネジメントの最初のステップです。次に、「コントロール施策の有効性を管理する考え方」を導入して、選択されたコントロール施策に対し、重点管理目的を設定します。筆者らがある企業にこの考えを適用したケースでは、約130のコントロール施策に対し、約80の重点管理目的を定義しました。その一部を抜粋した表3を参照してください。

さらに、こうした重点管理目的をその管理対象によって「個人単位」「部門単位」「システム単位」「情報資産単位」の四つに分類し、重点管理グループを構成します。

この重点管理グループごとに、企業の状況に応じて管理目的を選択して、具体的な管理プログラムに展開します。結果として、マネジメント体系は、こうした管理プログラム群で構成されることになります。

このような管理プログラムにまとめ上げることにより、経営としての優先順位や戦略課題との整合性の確認などがプログラム単位で可能となり、企業変革の視点で全社員の意識改革につながるセキュリティー教育などを重要な管理プログラムとして浮かび上がらせることもできます。

コントロールとマネジメントを分解し、マネジメント体系としてこのようにまとめ上げることにより、高度のスキルや経験を必要とする活動を管理プログラムとして集中化することが可能となり、数少ないセキュリティー人材の有効活用が図れるという側面も出てきます（図7）。

4.5. 組織体系

セキュリティー・マネジメントを実施する組織体制の検討には、まず組織のラインとスタッフとの関係を明確にしなければなりません（図8）。

これまでのセキュリティーは、ある特定の専門家の仕事として理解されていたため、セキュリティーを守るのは担当のスタッフ部門の責任であると理解されていた節があります。しかし、これからの時代は、セキュリティーを守る責任と事業を遂行する責任とは一体不可分になります。事業運営に情報は欠かせない資産であり、その安全が保たれなければ、事業責任者としての義務が果たせないことになります。

すなわち、ラインには、その権限や責任の中にセキュリティーの確保が当然のごとく含まれていると考えるのです。スタッフは、ラインがこのような権限や責任を遂行するための基準を示し、ガイドしてレビューをする役割を担うことになります。スタッフがラインの責任や権限の一部にまで手を伸ばす状況をよく

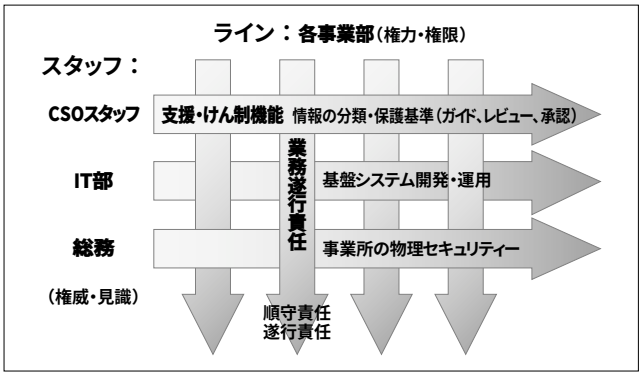


図8. ラインとスタッフの関係

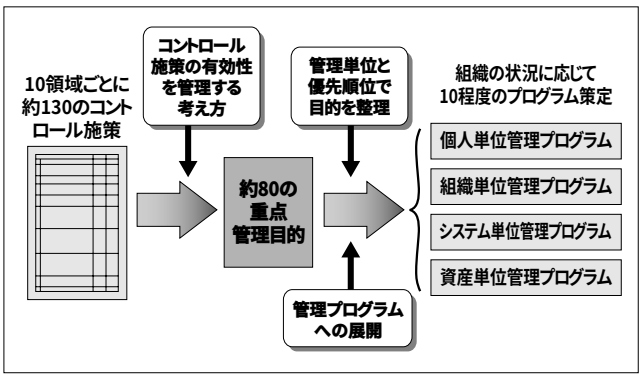


図7. マネジメント体系検討の手順

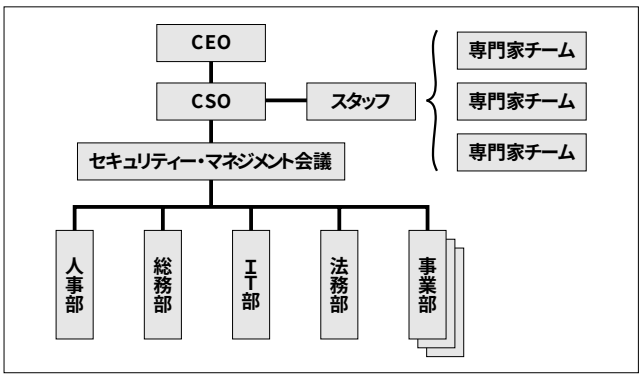


図9. CSOを中心とする体制

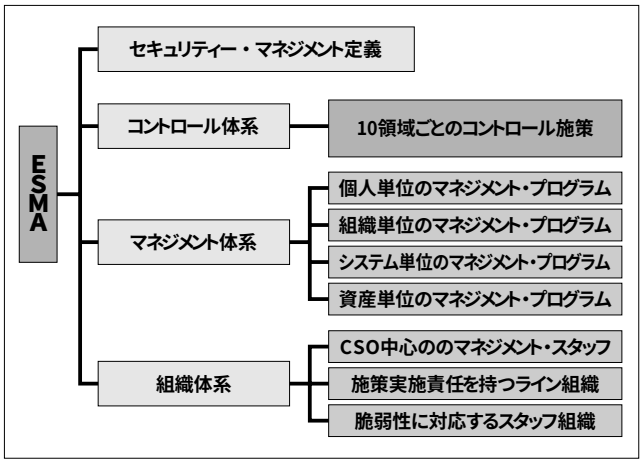


図10. ESMAの構造

見聞きしますが、本来の責任分担をあいまいにするようなスタッフの権限拡大は、望ましくありません。ラインがスタッフの定めた基準やガイドに従うためには、スタッフに権威や見識がなければならないと考えるべきでしょう。スタッフに権限がないからラインに徹底できないと嘆くのではなく、権威や見識が足りないと反省すべきです。

ESMAの体系でいうと、ラインがコントロールの実施を担当し、スタッフがマネジメントの実施を担当するのが基本になります。ただし、各ラインでバラバラにやると効率の悪いコントロールもあるので、その場合は集中化して実施した方がよいコントロールを集めて、特定のスタッフ部門が担当する場合もあり得ます。その場合も、ラインから委託されてスタッフが実施しますが、責任はラインに残ることを明確にしておく必要があります。

企業の中で、セキュリティー・マネジメントを推進する核はCSOです(図9)。CSOは、企業のセキュリティー・マネジメント全体を統括し、ラインとスタッフが効果的に連携し、協調し、時にはけん制し合う関係を作らなければなりません(図10)。

そのためには、CSOを支えるスタッフに、セキュリティーの知識や技術に長けた人材を配置し、全社のセキュリティー・マネジメントの核としての権威と見識をつくり上げなければなりません。また、各組織の代表者で構成されるセキュリティー・マネジメント会議は、全社統一的に実施しなければならないコントロール策の決定などの重要な役割を果たす討議機関であり、意思決定機関です。

本社スタッフ部門は、例えば人事部は人にまつわる脆弱性(ぜいじゃく)にいかに対抗するかを企画する意味で、セキュリティーの担当スタッフ部門としての役割を担うとともに、情報を使って業務を遂行する1ライン部門としての性格も併せ持ち、両方の立場から対応していかなければなりません。

4.6. ESMAの全体像

ESMAは、結局大きく四つの要素から構成されることになります(図10参照)。

5. 企業経営におけるセキュリティー・マネジメントの意義と価値

企業が、4.6節の図10で紹介した四つの要素をESMAの体系としてまとめ上げることにより、2章で指摘したセキュリティー・マネジメントの四つの課題が解決可能であることを確認しておくことにします。

(1)の「個人の意識や企業文化の変革の側面」については、ESMAという発想自体からして、そのことを意識してセキュリティー・マネジメントの定義に明確に宣言されなければなりません。個人単位、組織単位のマネジメント・プログラムにそれらが色濃く表れてくるでしょうし、CSOを中心とするマネジメント・スタッフに、その改革のシンボル的な役割が期待されるでしょう。

(2)の「マネジメント部分の欠如」については、ここがそもそもこのアーキテクチャーの発想の原点でもあり、マネジメント体系を明示して各種のマネジメント・プログラムを展開することで解決できなければなりません。

(3)の「人材配置や活用」については、本質的に人材不足や育成が難しいという点はありますが、組織体形の中でCSOスタッフに専門家チームを編成し、ラインとスタッフの関係を明確に整理したことにより、配置などの難点はかなりの部分が解決できるはずです。人材の育成という点では、企業内のキャリア・パスの問題やコア・コンピタンスとどう関係するかなど、本質的な議論が残り、これらはアウトソースの検討にゆだねます。

(4)の「責任の所在の明確化」については、コントロールとマネジメントを分解してそれぞれに管理サイクルを定義し、ラインとスタッフの基本的な関係に基づいて責任分担を定めることによって解決できます。

ここで紹介したセキュリティー・マネジメントの考え方のベースは、当初はITのセキュリティーから始まり、ITにとらわれない情報全般のセキュリティーへと発展してきました。本論文で展開した検討のほとんどは、さらに企業が直面するそのほかのセキュリティーへの適用も可能な汎用性を備えています。

最近は、多くの企業がCSOを指名するようになってきました。実際にそうした人たちの意見を聞くと、当面は情報セキュリティーが中心だが、そのほかのセキュリティーに責任がないわけではないと認識されています。従って、企業がこれからつくり上げ

るセキュリティー・マネジメントの枠組みには、暗黙のうちに、情報のみならずそのほかのセキュリティー・マネジメントにも適用可能な広がりが求められているといえるでしょう。その意味でも、本論文で提唱するESMAの価値は高いと思われます。

6. セキュリティー・マネジメントのアウトソーシング

ESMAにより、これまでは考えられなかったセキュリティー・マネジメント分野にも、ビジネス・プロセス・アウトソーシングの考え方が適用可能になります。

これまで、セキュリティー・マネジメントは特に結果指向が強く、極端にいえばどんな方法を採っても、結果として事故さえ起きなければよいという風潮がありました。そのため、どんなにうまくやっていても、一部の不心得者が事故や事件を起こすと、すべての努力が水の泡と消えることにもなりかねません。一方、何もしていなくても、事故さえおきなければ評価されます。これでは、まるでギャンブルです。このような世界には、アウトソースという発想のビジネスは困難です。

しかし、ESMAの考え方で企業のセキュリティー・マネジメントを整理すると、そこには明確にマネジメント・アウトソースという形態で、委託する側と委託される側の双方にメリットのあるビジネスの構図が浮かび上がります。

企業が自社のコンピタンスに特化しながら、セキュリティーに関する核心の意思決定をマネジメント・チームが確保しつつ、先進的なセキュリティー知識や技術を必要とする部分は、的確に外部の力を借りて、確固たるセキュリティー・マネジメントを確立することができるようになります。

具体的には、企業のCSOを支援するスタッフ・ファンクションのマネジメント体系に定められた業務の委託を受けるのです。この中には、有効なコントロール施策の検討から、その実現のための実施責任の配分、進捗状況の確認、各種のセキュリティー教育や啓発キャンペーンの企画と実施、定期的な点検や監査の実施、擬似ハッキングによる検証、システムの開発過程におけるレビュー・プロセスへの参画、あるいは事業所の物理的な管理策の検討、入退室管理や所持品検査など、およそセキュリティーに関連するあらゆるものの企画と検証機能が含まれることになります。

さらに一歩進めて、本来ラインが実施する責任のあるコントロールのうち、集中して実施した方が効果の高いコントロールをまとめて委託を受けることも可能です。

これは、アウトソーシング事業から見ると、従来のITやセキュリティーの経験、マネジメントの枠組みを背景に、新たなビジネス・プロセス・アウトソーシングとしてのセキュリティー・マネジメント・アウトソースのサービスが可能になる道を示すことにもなります。

企業のマネジメント層に対して、IBMの総合力を背景に、より価値の高いサービスを提供できる道を開くことをも意味します。

7. おわりに

e-ビジネスの時代を迎えて、セキュリティーの重要性は今さら繰り返すまでもなく、多くの企業がその確立に取り組みつつあります。国際的な標準化も進んできましたが、残念ながらまだ満足できる状況にまでマネジメント・レベルが向上したといえる状況ではありません。

2002年7月に、経済協力開発機構（OECD）が10年ぶりにセキュリティーのガイドラインを改訂しました。その改訂の中心は、この10年間に起きたインターネットを中心とするネットワーク環境の大きな変化によるものです。これまでは、責任の原則、いわゆるアカウンタビリティーの確立が第一の原則でしたが、今回の改訂で順序が入れ替わり、認識の原則、情報の利用者すべてにアウェアネスを高めることが第1原則とされました。

同時に、“ Culture of Security ”の概念が導入されました。日本語で言えば、さしずめ「教養としてのセキュリティー」が全員に求められることを意味していると理解すべきでしょう。このことも、現在の企業が置かれている経営環境と、求められているマネジメントを明確に示しています。

このマネジメント・アーキテクチャーの採用により、企業の情報を中心としたセキュリティーから人材やそのほかの経営資源も含む、いわゆる企業の安全を確保する包括的なセキュリティー・マネジメント確立の一助になれば幸いです。

（ページ数および表記上の観点から、著者の了解を得て編集部にて手を入れてあります）

[参考文献]
[1] 高梨 智弘『リスク・マネジメント入門』日経文庫
[2] 国際会計士連盟報告『企業価値を向上させるビジネスリスク・マネジメント』東洋経済新報社、2000年
[3] 三菱総合研究所政策工学研究部『リスクマネジメントガイド』日本規格協会、2000年7月
[4] アンダーセン/朝日監査法人『図解リスクマネジメント』東洋経済新報社、2001年5月
[5] 東京海上火災保険企業リスクコンサルティング室『図説企業リスクのすべてその事例と対策』東洋経済新報社
[6] 花井 荘輔『リスクアセスメントメント ヒューマンエラーはなぜ起こるか、どう防ぐか』丸善、2000年9月
[7] 長谷川 俊明『リスク・マネジメントの法律知識』日経文庫、1999年2月
[8] 後藤 正彦『緊急事態を乗り切る企業のリスク・コミュニケーション』日本能率協会マネジメントセンター、2001年5月
[9] 松本 俊次『リスク・マネジメントで会社を守れ』工業調査会、1999年6月
[10] アイアン・ミトロフ『危機を避けられない時代のクライシスマネジメント』徳間書店、2001年10月
[11] 大木 栄二郎『経営戦略としての情報セキュリティー』工業調査会、2001年7月
[12] P・バーンスタイン『リスク　神々への反逆』日本経済新聞社、1998年8月
[13] 大藪 俊一「こうすれば会社は変わる―Change Management ―」『PROVISION』No.33、日本アイ・ビー・エム、2002年
[14]‘ Information Security Management Part-1: Code of Practice for Information Security Management ’BSI, 1999
[15]‘ Information Security Management Part-2: Specifications for Information Security Management Systems ’BSI, 1999
[16]「ISO/IEC-17799 Code of Practice for Information Security Management」日本規格協会、1999年
[17]「ISO/IEC-TR-13335 Guidelines for the Management of IT Security（GMITS）：Part 1 - Concepts and Models for IT Security」日本規格協会
[18]「ISO/IEC-TR-13335 Guidelines for the Management of IT Security - Part 2：Managing and Planning IT Security」日本規格協会
[19]「ISO/IEC-TR-13335 Guidelines for the Management of IT Security - PART 3：Techniques for the Management of IT Security」日本規格協会
[20]『ISMSガイド（Ver.1.0）』（財）日本情報処理開発協会、2002年4月
[21]『ISMS認証基準（Ver.1.0）』（財）日本情報処理開発協会、2002年4月