企業統治に欠かせない情報セキュリティの実装

Implementation of Information Security Required for Corporate Governance

長谷川　幸成

要　約　個人情報保護法の施行に向け，業種を問わず多くの企業が，その対策に追われている．セキュリティが実装されていれば，法律が施行されたからといって対応に追われることはないはずであるが，残念ながら国内のほとんどの企業はセキュリティを固定的なコストと認識しており，事前にあるいは積極的に投資をする対象としていないのが事実である．しかし，この法律の施行をきっかけに企業の経営者達は，セキュリティを実装するだけでなくガバナンスの一翼を担うことに気づき始めたのである．自社の守るべき情報資産を選定し，ISMS（情報セキュリティマネジメントシステム）のフレームワークを構築して情報セキュリティのベースラインを上げることにより，ガバナンスの効いた経営が可能となる．

本稿では，ISMS 構築のポイントを紹介しつつ，情報セキュリティとガバナンスの有効性について説明する．

Abstract　Many of the Japanese companies are now very keen to implement quite a few measures for “Privacy Information Protection Law” to be fully effective coming April. The company, where information security action is well put in place, does not have to be in a hurry, however, such “security compliance” is perceived as a fixed cost and almost every firms unfortunately didn’t have intended to aggressively invest on. Now, by this law effective next year, the top management has come to notice that the security measures are valid not only for the law but also for the corporate governance. “Good Governance Company” can be realized by the information security actions, such as selecting information assets to be protected, ISMS（Information Security Management System）framework development and leveraging the security level.

In this article, the information security and governance will be discussed according to the ISMS guideline.

1. はじめに

2005 年 4 月に施行される個人情報保護法をはじめ，セキュリティ関連の法制度の整備が進み，企業はこれらの遵守・準拠を求められている．万一，個人情報や営業秘密などの情報漏洩が発覚した場合には，企業の信用の失墜だけでなく経営自体にも多大な影響が及ぶからである．

一方，情報セキュリティはビジネスを進める上での重要な要素であり，ガバナンスを構築する上でも必要であるとの認識が企業の間にも定着しつつある．また，中央官庁の入札には，プライバシーマークや ISMS 認証の取得企業であることが条件であったり，ステークホルダに一定レベルの情報セキュリティを求める企業も増えてきていたりと，情報セキュリティの実装が他社との差別化やビジネス拡大に結びついている．

これらを背景に，多くの企業が情報セキュリティ対策に積極的に取り組み始めている．企業の情報セキュリティに対する取り組みが必要な要因を図 1 にまとめた．

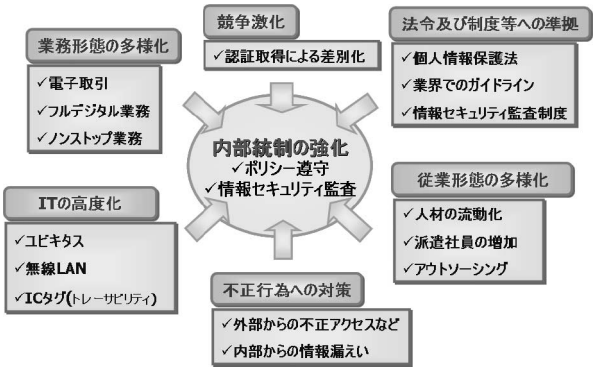


図1　企業を取り巻く環境の変化

- 法令及び制度等への準拠
  1. 2005年4月1日施行される個人情報保護法への対策
  2. 経済産業省が推進する情報セキュリティ総合戦略，情報セキュリティ監査制度への対策
  3. その他業界ガイドラインへの準拠など
- 従業形態の多様化
  委託先企業からの個人情報漏洩事件が増えたことからも理解できるように，従業員だけでなく派遣社員や委託先の厳重な管理も必須である．
- 不正行為への対策
  不正行為には，インターネットからのハッキング行為や施設・設備への物理的な侵入による外部からのものと，権限のある者による持ち出しなど内部からのものがある．対策としては，ネットワークや施設・設備を要塞化することに加え，論理的アクセス権限や情報の管理の見直しなど内部者の不正行為防止対策が必要である．また，巧みに情報を引き出すソーシャル・エンジニアリング対策として，従業員への情報セキュリティ教育も必須である．
- IT の高度化
  IT が高度化するにつれ，脅威や脆弱性も大きくなってきている．そのための対策はIT の進化と比例させなければならない．
- 業務形態の多様化
  紙文書から電子文書へのフルデジタルな業務への移行が進んでいる．その影響によりノンストップの業務が増えたため，事業を継続させることが企業の必要条件となった．その可用性を確保するために，情報セキュリティの実装が必要となる．
- 競争激化
  競合他社がセキュリティ関連の認証を取得してブランドを構築するなど，差別化を図る企業が増えている．
- 内部統制の強化
  外部環境の脅威による情報漏洩は全体の2割であり，残りの8割が内部環境の脆弱性を起因として発生している．対象となる情報利用者に対しての管理面，システム面における対策が最も重要である．

本稿では，情報セキュリティの実装を推進することにより，企業のガバナンスを確立することが可能であることを，ISMS を構築するプロセスを紹介しながら，経営への有効性として提言する．

2.　経営者の責務

企業の経営者は，戦略的で分析的な視点からセキュリティのプランニングを行い，施策の優先順位を決定する責任がある．また，経営者には企業のステークホルダーや社員に対してセキュリティ投資の妥当性や効果を理解させる政治的な手腕やコミュニケーション能力も求められる．今後は情報セキュリティや個人情報保護に関する法規制が，企業のセキュリティ戦略に大きな影響を与えることになるため，経営者は，こうした法規制に対処するための有効な施策を立案しなければならない．これらを遂行するうえでは，業務部門のビジネス・フローを徹底的に調査して，それぞれのフローが法規制に抵触する可能性があるかどうかを綿密に分析する必要がある．

このようにセキュリティはコーポレート・ガバナンス，あるいはリスク管理の視点に立脚した新しい取り組みの一つとして捉えなければならない．当然，この取り組みは，経営者の企業理念を起点にスタートさせる必要があり，その理念に基づいて具体的なセキュリティ対策の方針や手順を体系化し，派遣社員やアルバイトも含めた全従業員にそれらの遵守・遂行を徹底させなければならない．

3.　情報セキュリティの定義

情報セキュリティは，情報や情報システムを安全な状態にすることである．一般的に情報セキュリティは，「情報の機密性*1，完全性*2 および可用性*3 を確保し，維持し続けること」と定義されているが，この三つの要素を満足している状態を安全な状態という（図 2）．

1992 年の「OECD 情報セキュリティガイドラインに関する委員会勧告」（Recommendation of the Council concerning Guidelines for the Security of Information Systems（adopted by the Council at its 793 rd Session on 26–27 November 1992））の付属文書「情報セキュリティガイドライン」（Guidelines for the Security of Information Systems, 26 November 1992, 以下 OECD ガイドラインという）では，情報システムの機密性，完全性および可用性を阻害する危害から情報システムを保護することを情報システムセキュリティの目的としている[2]．

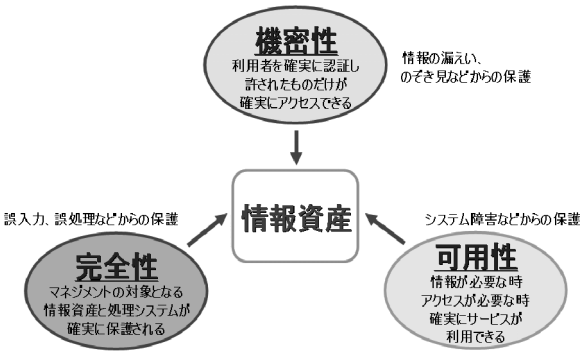


図 2　情報セキュリティの定義

4. 情報セキュリティマネジメントの必要性

情報セキュリティマネジメントは，単なるセキュリティ技術の問題ではなく，情報を企業にとって価値のある情報資産として捉え，それを管理する企業経営の取り組みである．その構築は，情報資産が持つリスクを識別し，許容範囲外のリスクに対し，どう対処するのかをマネジメントするフレームワークを確立し，計画（PLAN）⇒実践（DO）⇒チェック（CHECK）⇒計画修正（ACT）の PDCA サイクルに従いセキュリティを向上させることである（図 3）．

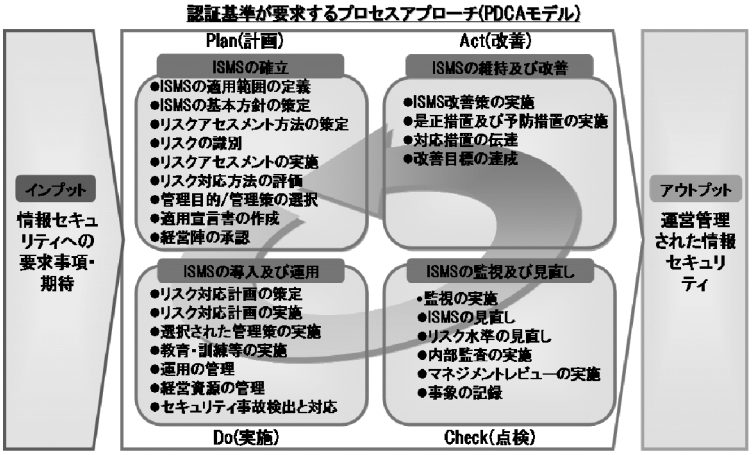


図 3　PDCA モデル

リスクとは，「企業の事業目標の達成に影響を与える不確実性」をいう．組織の財務上のリスク，取引先の信用リスク，従業員の事故，生産設備被災，環境リスクなど多様なリスクがある．経営の立場から見ると，企業活動を阻害する要因が情報資産に直接かかわるリスクであっても，直接かかわらないものであっても，企業活動に支障を与える事態そのものに違いがあるわけではない．

組織の事業目標を達成するために，情報資産にかかわるリスクと直接かかわらないリスクの両輪を踏まえた ISMS の実装が必要である．企業においてこれらのリスクを情報セキュリティの観点から MECE 的に表すと，図 4 セキュリティ体系図になる．

企業の経営者は，物理的セキュリティからコンプライアンスまで事業を継続するために必要な要素全てに対して ISMS を有効に適用しなければならない．

5. ISMS（情報セキュリティマネジメントシステム）の実装

日本情報処理開発協会(JIPDEC)は ISMS 適合性評価制度を設け，ISO/IEC 17799 や BS 7799 を参考にして情報セキュリティにおける認証基準を策定している．ISMS 適合性認証制度は，情報及び情報処理施設などを対象とした ISMS を構築することを目的としており，他の ISO が推奨するように PDCA サイクルを継続的に運営していくことによって組織のセキュリティレベルをより確かなものにしていく制度である．

ISMS を構築することによって，情報セキュリティの側面から企業のガバナンスの構築が可能となる（図 5）．

日本ユニシス（以下，当社）では，日本の IT 業界で始めてシステム監査部門を立ち上げる

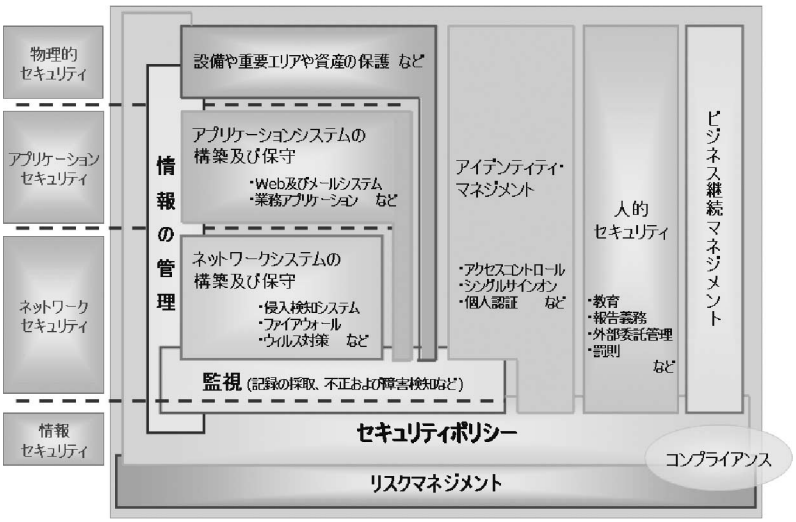


図 4　セキュリティ体系図

など，早くから IT 構築および運用に対する情報セキュリティの重要性に着目してきた．また，ISO/IEC 17799 および BS 7799 をもとにこれまで培ってきた当社の情報セキュリティの概念を融合し，世界で初めてアウトソーシング事業での BS 7799 認証取得も成し遂げた．これらの成果を成し遂げた当社のコンサルティング・サービスのノウハウより ISMS を構築するためのポイントを述べる．

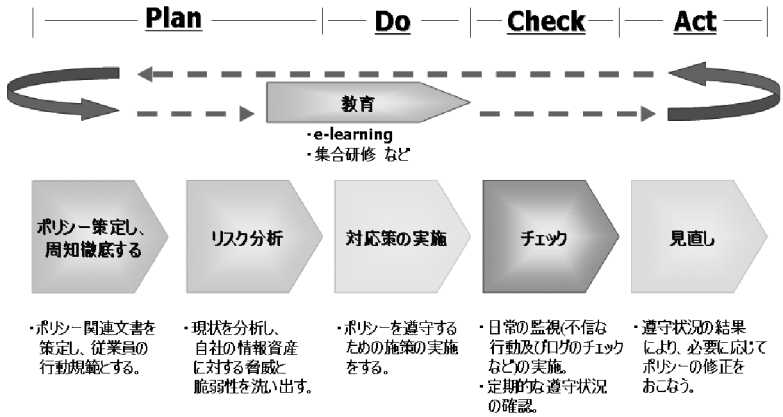


図 5　PDCA サイクルで運営する ISMS 運営

5.1　情報セキュリティポリシー

情報セキュリティポリシーが，経営者の承認により定められていることが肝要である．情報セキュリティを実装する上で情報セキュリティポリシーは情報利用者のよりどころであり，企業のセキュリティの基本的な方針を示すものである．また，この情報セキュリティポリシーを策定する上で重要なことは，PDCA のフレームワークが構築されていることである．すなわち，この情報セキュリティポリシーが策定されれば，情報利用者は自分自身が何をすべきかが明確になる．

企業の多くは総務部の策定した文書管理規程と情報システム部の策定した電子情報管理規程による運用をされているが，電子文書と紙文書を一つの情報として捉え，その情報の重要度によって管理することが情報利用者にとっては分りやすく，管理者にとっても管理しやすい体系となり，PDCA の構築，すなわち企業のガバナンスが容易になると考えられる．図 6 に理想的な情報セキュリティポリシーの体系図を示す．

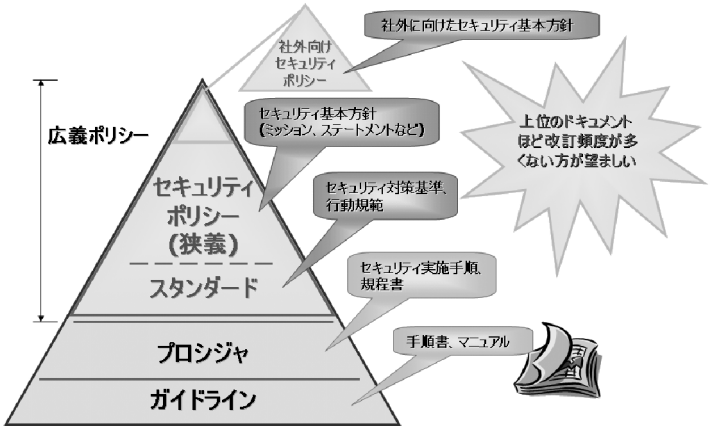


図 6　情報セキュリティポリシーの体系図

5.2　情報セキュリティ組織と体制

ISMS のフレームワークを実装するためには，組織横断型の体制の構築が必須である．情報セキュリティマネジメントシステムを推進する組織が情報システム部に偏った組織であったりすると，情報システム部の良識の範疇でしか情報セキュリティ対策が行われなくなる．

また，ISMS のフレームワークを推進するためには，それを推進するための専任の組織も必要である．情報セキュリティポリシーは策定したが，PDCA のフレームワークが回っていないと情報セキュリティレベルは下がる一方である．

推進する組織と体制が編成されたら，その組織内での牽制を効かせることが肝要である．一握りの権力者の下で実装された ISMS は封建的なシステムであり，その組織自身が企業にとって最も脆弱なものである．その他に考慮すべきこととして，関連会社や委託先の代表者も運営組織に参加させることが大切である．これにより，ISMS が情報を利用するすべての者によって構築されることになる．

5.3　情報の分類と管理

情報の分類方法は，日本の多くの企業では，①極秘，②社外秘，③一般のような 3 段階で定められている．しかし，分類区分が多ければ，管理をするための費用と労力を要する．情報が情報利用者にとって管理しやすいように，分類も簡素化することが情報セキュリティマネジメントシステムの構築に役立つのである（図 7）．

5.4　外部委託管理

外部委託は，企業の経営において，コスト削減のためにはなくてはならない手段と言える．

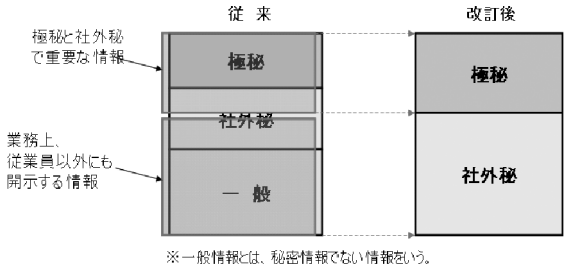


図7　情報の分類について

しかし，その反面，就業規則などの強制力がないため，適切に管理されない場合には脅威となり得る．企業は，これらの脅威に備え，予め委託先事業者を選定する基準を定めておかなければならない．以下にその因子を示す．

・安定性（売上，利益，事業内容等）
・セキュリティ対策状況（特に個人情報の取り扱い）
・受託実績
・技術レベル
・委託先のシステム環境
・委託費と支払条件
・再委託の有無
・セキュリティ事故時の監査権行使
・セキュリティ事故時の責任範囲

5.5　人的セキュリティ

経営者は,情報セキュリティの脅威および懸念に対する情報利用者の認識を確実なものとし,情報セキュリティポリシーを維持していかなければならない．そのためには，事業における情報セキュリティの必要性や導入するISMS構築の必然性についての認識が必要であり，それを各個人の姿勢や行動に結びつける「意識付け教育」や組織の構成員としての「コンプライアンス教育」が重要となる．

また，セキュリティ教育は会社としての義務でもある．情報利用者が誤って情報を漏洩してしまう危険性について事前に教育しておくことによって，セキュリティ事故の発生を減らすことも可能となる．

図8は，教育の展開方法を表している．留意すべき点は，情報利用者だけの教育ではなく，責任者や経営者が何をすべきか学ぶことである．

5.6　環境的セキュリティ

環境的セキュリティとは，情報資産の設置場所，管理状態，管理体制の脆弱性に対処し，情報資産の環境面での脅威から生じるセキュリティリスクを抑制することを意味する．

具体的な例としては，打ち合わせ専用のフロアや荷物などの受渡し場所を設置し，執務室あるいは事務所への第三者の侵入を無くすことによって脆弱性を軽減し，外部からの脅威に対処することが必要である．

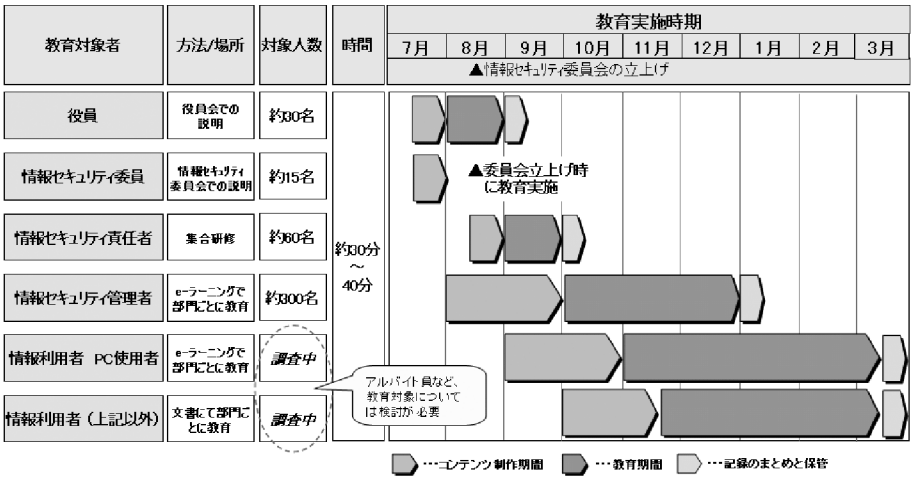


図 8　セキュリティ教育計画

5.7　技術的セキュリティ

技術的セキュリティとは，情報システムに実装したセキュリティ機能を利用してコンピュータ犯罪やネットワーク犯罪の発生を抑制する論理的セキュリティを意味する．

ISMS を構築する上で，情報利用者への教育など管理面に投資をするか，次に示すようなシステム面を整備することに投資をするかは，その企業の文化によって異なる．教育を行い情報利用者のリテラシを向上させればシステム対応などの投資は軽くなり，逆にシステム対応がしっかりされていればある程度は管理面での許容が可能になる．脆弱性を減少させる効果を考えた場合，管理面への投資とシステム面への投資はバランスよく行われることが好ましいと考えられる．下記に技術的セキュリティとして考慮すべき管理策を示す．企業は，これらの該当する管理策について何らかの投資が必要となる．

1)　通信および運用管理
- ・運用手順および責任
- ・システム計画の作成および受け入れ
- ・不正ソフトウェアからの保護
- ・情報システムの管理
- ・ネットワークの管理
- ・媒体の取扱およびセキュリティ
- ・組織間における情報およびソフトウェアの交換

2)　アクセス制御
- ・アクセス制御に関する事業の要求事項
- ・ユーザアクセス管理
- ・ユーザの責任
- ・ネットワークのアクセス制御
- ・オペレーティングシステムのアクセス制御
- ・アプリケーションシステムのアクセス制御
- ・システムアクセスおよびシステム使用の監視
- ・モバイルコンピューティングおよび遠隔地勤務

3） システムの開発およびメンテナンス

・システムのセキュリティ要件事項

・アプリケーションシステムのセキュリティ

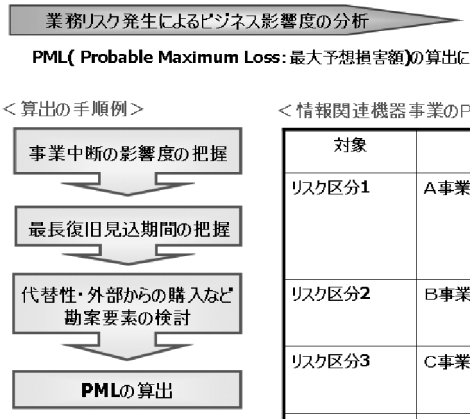
・暗号による管理策

・システムファイルのセキュリティ

・開発およびサポートプロセスにおけるセキュリティ

5.8 事業継続性

システム障害や自然災害などによって情報システムやサービスが停止し，業務が中断するような事態が生じた場合，速やかに復旧し，業務を継続しなければならない．このような事態を事前に想定して，業務を継続するための管理策を検討し，整備して維持する必要がある．有事に備えて事前に図9に示すような業務リスク分析によるリスク管理を行うことによって，限度を越えない有効な投資を実現することが可能となる．



＜情報関連機器事業のPML算出例＞

対象		算出式	損害額
リスク区分1	A事業所	総生産高8410億円×影響度80%×最長復旧期間6ヶ月／12ヶ月	3364億円
リスク区分2	B事業所	8410億円×60%×6ヶ月／12ヶ月	2523億円
リスク区分3	C事業所	8410億円×60%×6ヶ月／12ヶ月	2523億円
構外ユーティリティ	電気	8410億円×100%×1ヶ月／12ヶ月	700億円

図9 業務リスク分析

5.9 法令遵守

企業は，情報システムの設計や運用，利用および管理においては，法的な要求事項を満たさなければならない．具体的には，関連法令・規制，契約上の義務，ならびにセキュリティ上の要求事項への準拠が必要である．

個人情報保護法においても，施行前にそれぞれの業界のガイドラインに従って各企業が必要な対策を適用している．

6. 情報セキュリティ実装上の留意点

6.1 情報活用の利便性

情報セキュリティ確保のために，情報へのアクセス権限を細かく設定するケースも多く見受けられる．しかし，そのために必要な情報にアクセスするのに手間も時間もかかり，情報のスピィーディな活用が阻害され，業務効率や生産性の低下を招いているという例もある．スムーズな情報活用と情報セキュリティの確保は二律背反な面を持つが，そのバランスは考慮する必

要がある．

6.2　体系的な対策の実践

システムなどのハード面での対策は容易に対応が可能である．しかし，人的な管理，社員の意識改革といったソフト面での対策はなかなか困難であり，情報セキュリティ教育を徹底するとともに適切なチェック体制を確立することも必要である．そのためには，情報セキュリティ対策全体を主導する権限と責任を有する組織を設置するのが効果的である．

6.3　リスクマネジメントとの融合

情報セキュリティの実装をする際，情報セキュリティマネジメントとリスクマネジメントを全く違うものであると認識している企業が多い．参考文献[1]経営戦略としての情報セキュリティでは次のように説明している．

情報セキュリティマネジメントの中にも，リスクの分析やその対応，危機管理などが含まれ，またリスクマネジメントの中にも情報セキュリティ対策などが含まれる．情報セキュリティとは情報の安全を守る立場でものを見ているのに対し，リスクとは危険側から見ている．局部的には同じものを反対側から見ており一見裏表の関係にあるように見えるが，その局部から全体へと考えを広げていくと，お互いが他を包括する関係にあることがわかり，実は全く同じことなのである．このことから，これらを担当するプロジェクトが融合し，効率的に対策を実施することが望ましい．ほとんどの企業では全く別の管理組織として運営されている．

6.4　外部認証取得の効果

IT 革命の時代には，情報のセキュリティの確保がビジネスの世界では極めて重要である．自社の情報セキュリティの確保に，それぞれの企業は戦略や経営課題の優先順位に応じて対応を始めている．ステークホルダーも取引企業を選択するために，その企業での情報セキュリティマネジメントのレベルがわからなければ信頼につながらない．

信頼の確立，ビジネス機会の拡大のために，企業全体の情報セキュリティマネジメントの有効性を客観的な基準に基づいて審査し認証しようという動きがある．BS 7799 や ISMS 認証制度がこれにあたる．具体的には，企業内の情報セキュリティの管理全般にわたるマネジメントシステムを審査の対象とし，国際的な共通の基準に基づいて的確なセキュリティマネジメントが継続的に行われていることを，権威のある機関が認証し登録するものである．この考えや仕組みはこれまで品質管理や環境管理に用いられてきた ISO 9000 や 14000 の認証と同じであり，これらの手法を情報セキュリティにも適用しようとするものである．図 10 に外部認証取得を考えた際の計画例を示す．図 10 の外部認証取得に向けてのマスタープラン案からもわかるとおり，外部認証取得のためには十分な準備と認証取得後の運用も考慮する必要がある．

6.5　セキュリティ事故後の対応

セキュリティ事件が後を絶たないが，自社が情報漏洩などのセキュリティ事故を起こしてしまったらどうすべきか，事前に ISMS を構築して対処している企業は少ないのが事実である．事故後処理として必要な対処を次に示す．

1)　マスコミ対応

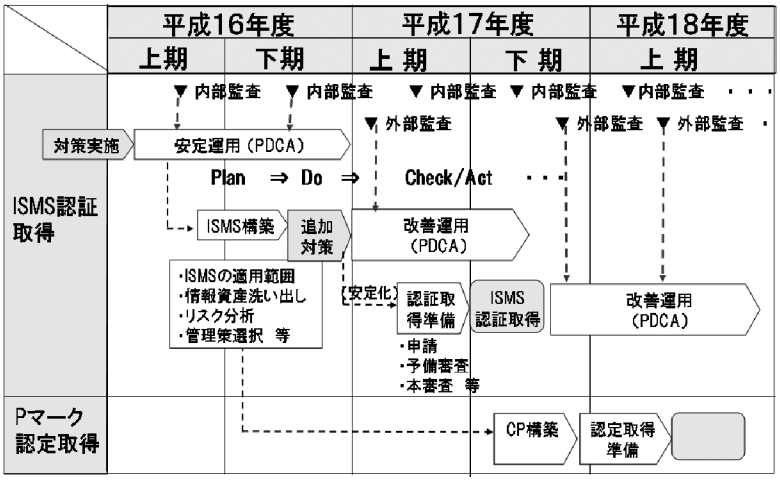


図 10　外部認証取得に向けてのマスタープラン案

・対策本部の設置など

2）　ステークホルダー対応

・従業員，取引先への対処など

3）　リカバリー対応

・短期，中長期対応の実施

リカバリー対応においては，図 11 に示すとおり管理的対応と技術的対応を短期および中長期対策として全ての関係者に周知された上で確実に実施することが肝要となる．マスコミやステークホルダーがこれら具体的な対策を知ることにより，セキュリティ事故にも迅速に対処し得る企業の姿勢が信頼を回復する一役となるからである．

	必須対策	対応方法
組織的対策	・情報セキュリティ責任者CISO、プライバシー責任者CPO任命。 ・情報セキュリティ基本方針、ポリシーの作成/方針の開示。 ・組織横断的な情報セキュリティ委員会機能強化、組織別委員任命。	管理的対応
人的対策	・セキュリティ意識/モラル向上教育の実施、自己監査実施。 ・業務委託先契約の見直しもしくは守秘義務条項の強化。	
物理的対策	・入退館管理の強化。 ・M/C室情報管理の強化。 ・執務室におけるマネジメント強化。	
情報管理	・情報の取扱い方針策定（秘密情報の分類方法や情報のライフサイクル等） ・媒体の管理強化	
技術的対策 ●情報漏洩防止 ●不正アクセス対策 ●パスワード管理 ●障害監視	・情報漏洩防止ソフトの導入　・修正プログラムの自動適用 ・サーバのセキュリティ検査実施　・サーバの設定最適化 ・管理者権限パスワードの強化 ・システム監視、ネットワーク監視ソフトウェアの活用	技術的対応

図 11　短期的対応策例

7. お わ り に

CIO Magazine 米国版とプライスウォーターハウスクーパースが，2003 年 4 月 15 日から 7 月 7 日にかけて，世界各国の企業幹部や IT マネジャを対象としたセキュリティ対策に関する大規模な実態調査を実施した．その中で，2003 年の IT 予算に対する情報セキュリティ予算の

割合は，11% と報告されている．この投資の事実は，欧米企業が経営上情報セキュリティを必要不可欠なものと認めている証拠に他ならない．欧米企業は，セキュリティ対策に積極的に取り組んでおり，その累計の上に単年度のセキュリティ投資が考えられている．これに対し，日本企業は IT 革命の時代を迎えて，これから本格的なセキュリティ対策が始まろうとしている段階である．自社の情報資産に対するリスク分析が前提として存在し，その結果に応じてリスク対策としての投資効果を検討することが必要となる．現状においては，同業他社と比較して自社が極端に遅れていないことだけが経営者の関心であることが懸念される．

企業の投資は固定的な IT コストと機動的な IT コストに識別され，セキュリティは固定的な IT コストとして認識される（図 12）．このセキュリティに対するコストが最適化されていると，本来セキュリティに投資していたコストが戦略的コストとして利用することが可能となる．単純にセキュリティへの投資を抑えるのではなく，ISMS を構築して効果的な投資を可能とすることで，計画的なコスト管理が可能となる．

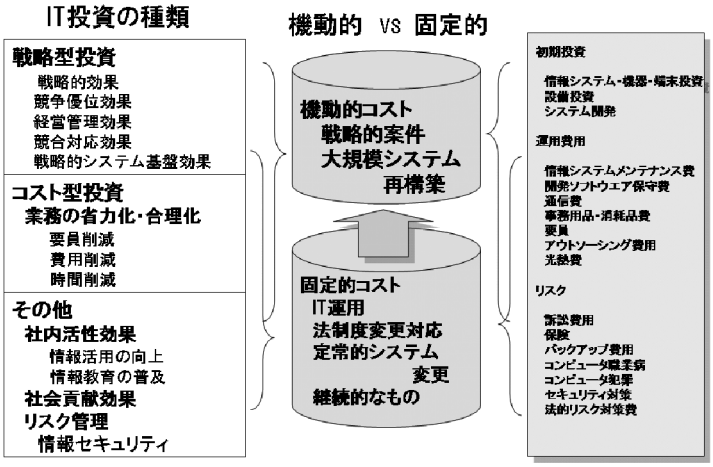


図 12　固定的 IT コストから機動的 IT コストへ

これまで情報セキュリティ対策は，企業の情報システム部門の問題として技術的に解決すべきものと位置付けられてきた．近年の IT 革命により，重要な経営課題であると認識されるようになりつつあるが，現実的には個別課題への後追い的な対応が主である．今後は，部門毎に個別課題への対応として個別に行われてきた情報セキュリティに関する意思決定を，将来のビジョンに沿って体系的に位置付け，各意思決定の相互間に整合性を持たせるガバナンスが必要となる．IT 革命により大幅に変化する情報の価値そのものの評価方法を確立し，その価値に見合う企業での管理体制を構築しなければならない．IT 革命時代の企業の信用力として，企業統治に欠かせない情報セキュリティの実装が問われることとなる．

＊1　**機密性**（confidentiality）：ISMS 認証基準では，機密性は「アクセスを認可された者だけが，情報にアクセスできることを確実にすること」と定義している．

＊2　**完全性**（integrity）：ISMS 認証基準では，完全性は「情報および処理方法が正確であることおよび完全であることを保護すること」と定義している．

＊3　**可用性**（availability）：ISMS 認証基準では，可用性は「認可された利用者が，必要なときに，情報および関連する資産にアクセスできることを確実にすること」と定義している．

参考文献　［1］大木　栄二郎，経営戦略としての情報セキュリティ，株式会社　工業調査会，2001年7月25日
［2］島田　裕次，榎木　千昭，山本　直樹，五井　孝，内山　公雄，ISMS認証基準と適合性評価の解説，株式会社　日科技連出版社，2002年11月12日

執筆者紹介　長谷川　幸成（Yukinari Hasegawa）
1990年日本ユニシス(株)入社．金融担当システムを経てEビジネスの推進プロジェクトに参画し，マーケットプレース決済，ICカード・金融業界のマーケティング，セキュリティのコンサルタントを経験．現在，エンタープライズ・ソリューション事業部ビジネスプランニング部セキュリティグループでセキュリティコンサルティングに従事．