セキュリティポリシー

青木　尚*

要　旨

電子商取引等いわゆるIT革命（情報革命）が情報化・ネットワーク化の進展を加速し，産業や政府活動の多くは，情報システムへの依存性をますます高めている。

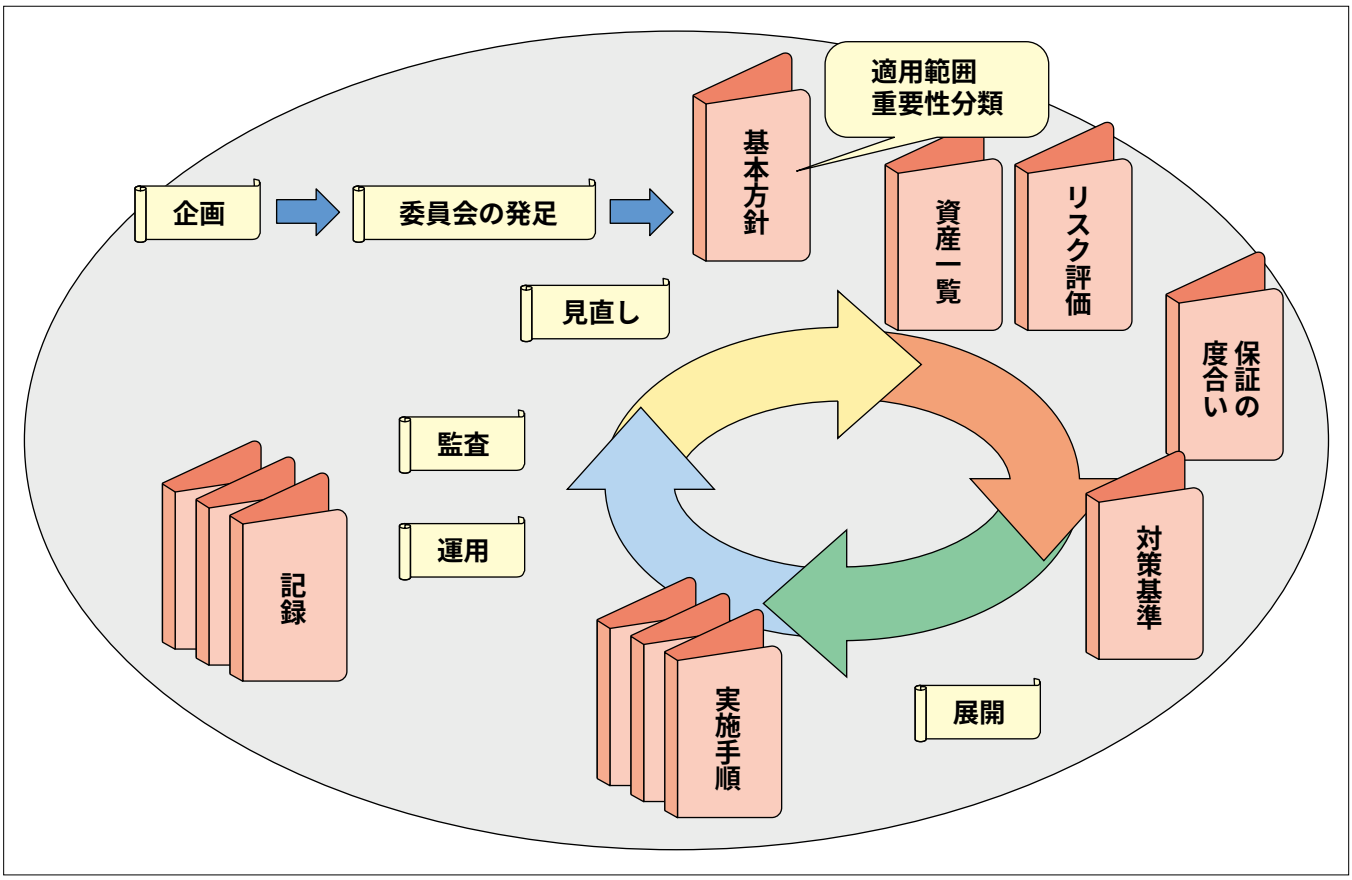
これに伴い，情報システムの安全面や信用面等から，情報システムを支える情報セキュリティの維持・向上が重要になってきた。

事実，コンピュータウィルスや踏み台攻撃等，情報及び情報システムは，その盗用，不正アクセス，改ざん，破壊，又は利用妨害などの脅威に常にさらされており，これに加えて，組織内部者の意図的な脅威についても無視できない。

これに対して，従来までは，入退管理，ウィルス対策，及びファイアウォールやIDS（侵入検知システム）等のシステムで対策してきたが，ここにきて，経営層・管理層の説明責任・危機管理，及び法的準拠性がクローズアップされてきて，組織や体制の下に総合的・体系的な管理を行う標準的なISMS（情報セキュリティマネジメントシステム）の導入が経営的に注目されている。

このような中，日本政府は，ISO／IEC17799（情報セキュリティ管理実施基準）の前身である英国標準BS7799等を参考に，「情報セキュリティポリシーに関するガイドライン」（2000－7）を発行し，省庁のセキュリティポリシー構築施策を展開した。また，金融庁も同様な施策を金融機関に対して行ってきた経緯がある。

現在は，ISMSの運用面の整備が行われており，例えば，㈶日本情報処理開発協会が2002年度以降の本格運用を目標にISMS適合性評価制度を準備している。



ISMS導入・運用プロセス

ISMSを導入し運用するには，例えば，情報システム管理部門などがISMSの導入を経営層・管理層に起案し，経営層・管理層の承認に基づいて組織全体の代表からなる委員会を発足し，策定するISMSの委員会決定と経営層・管理層の承認を取り付け，運用管理・見直し等を行うプロセスを経る。

*三菱電機インフォメーションシステムズ㈱