規範的セキュリティポリシへのISO規格などの適用について[1]

5W－5

杉野 隆
新潟国際情報大学

1. はじめに

ネットワーク運用におけるセキュリティポリシの重要性は，広く認識されている。しかし，セキュリティポリシが確実に実施されるためには，経営者の責務を含む企業としての意思を表明し，経営者，管理者をふくむ関係者の行動規範となりうる規範的セキュリティポリシの策定が重要である。規範的セキュリティポリシの策定方法論について，国際標準であるISO9000, ISO14000, 英国規格であるBS7799がフレームワークとして適用可能かどうか検討を行った。

2. 規範的セキュリティポリシの背景

インターネットの普及とともに，情報システムにおいてネットワークの利用が当然のこととなり，情報セキュリティ確保の重要性も認識されるようになってきた。しかし，具体的なセキュリティ対策の実施となると，日本の各組織の対応は遅れているといわれる。

そこには，

・セキュリティ対策関連製品は市場にあふれているが，適切な製品を選択できる技術力が不足している
・情報システム予算の総枠を絞られつつあるため，セキュリティ対策に投資する余裕がない
・セキュリティ技術者が不足している
・セキュリティ製品を導入しているが，専任管理者を配置する余裕がないため，日々の運用に手が回らない

などが原因として挙げられる。

また，重要なことは，セキュリティ対策のためのハード・ソフト投資がなされたかどうかではなくて，セキュリティ障害が起きたときに「いかにリスクを減らすようなプロセスが確立できているか」ということである。

セキュリティポリシ策定においては，個々の脅威に対抗するためのセキュリティ対策方針の決定とセキュリティ機能の導入運用を規定する記述的セキュリティポリシだけでなく，組織全体の行動規範を規定する規範的セキュリティポリシが，上記原因の解決のために重要である[1,2]。この視点からすれば，RFC2196[3]は記述的セキュリティポリシである。また，ISO15408「情報技術セキュリティ評価基準」[4]は，情報システム開発工程の中にセキュリティ設計プロセスを位置付け，想定される脅威に対抗するために必要なSecurity Objectivesの決定とその実現手段，及び評価基準をテンプレートとして設定したことに意義があるが，やはり視点は記述的セキュリティポリシにある[5]。

これらのセキュリティポリシのテンプレートには，セキュリティポリシないし対策を組織全体におけるPDCAサークルとして廻し，継続させていこうとする企業経営者のセキュリティマネジメントに対する意思表示が不充分である。

本論文では，経営者の責務までを含む規範的セキュリティポリシの策定方法論として，ISO9000, ISO14000, BS7799を対比して参照可能性を検討する。

2. ISO9000

ISO9000では，取引において顧客と供給者間で要求される製品/サービスの質は，製品やサービスの仕様だけでなく，質を生み出すプロセスに依存するとしている。そのために，製品やサービスの品質には言及せず，設計・開発から引渡しまでのプロセスの品質を顧客と供給者間の契約要件として明確にすることがISO9000の目的である。品質システムとしては，品質管理を行うための組織構造，手順，プロセス及び経営資源までを対象とし，行うべき管理要素を要求事項(ISO9001-9003)や推奨事項(ISO9004)として規定している。経営資源としては，人的資源ばかりでなく，設計・開発・生産関連の設備，情報システムなど，経営者の意思決定を必要とする要素が幅広く含まれており，情報システムのセキュリティシステム構築のためにも参考になる。

ISO9000 で規定している“経営者の責務”の対象を，“品質”から“セキュリティ”に言葉として置き換えてみると，情報セキュリティに関する経営者の責務は，「セキュリティポリシを作成し，セキュリティに関する業務を管理・実行する組織の責任と権限を明確にし，必要な経営資源を割り当て，管理責任者を任命すること」となり，まったく矛盾なく規定でき

---

[1] Applying ISO Standards to Normative Security Policies

Takashi Sugino E-mail:sugino@nuis.ac.jp
Niigata University for International and Information Studies
3-1-1 Mizukino, Niigata-City, Niigata 950-2292, Japan

る。セキュリティポリシは，作成されることに意味があるのではなく，確実に実施・見直しされねばならない。すなわち，組織の目的に則した行動規範の下で，実施できることから実行しながら次第にそのレベルを上げ，セキュリティ強度を上げていくという方策をとることになる。これには，組織にセキュリティへの関心の高まりを待つという意味と，セキュリティ脅威にどのようなものが出現するかは予め確定できるものではなく，その都度対策の強化とポリシへの反映を必要とするという意味がある。経営者は，この規範的セキュリティポリシにしたがって，情報システムのセキュリティ保護を実施することを組織全体に対して要求し，その実施に必要な経営資源（要員，設備，情報システムなど）の割当てを組織内外に対して保証することになる。

3 ISO14000[6]

環境保護に関しての，法規制に基づく管理モデルを構築し規則及び基準を守らない場合には処罰すればよい，という仕組みを作るだけでは環境劣化に確実に対処することはできないというこれまでの環境保護に対する経験に基づいて，ISO14001 は制定されている。各組織は，その環境側面を調べ，自らの目的と目標を確立し，効果的な信頼できるプロセスと継続的改善を誓約し，すべての従業員と管理者に指示して<環境マネジメントシステム(EMS)>を構築し，組織の環境パフォーマンスに対する責任と自覚を共有し高めるようにする。ISO14001 は，組織がこのような活動を継続して実施するための仕組みを PDCA というデミングサイクルとして構築することを求めている。
「品質方針」に相当する「環境方針」は，組織の EMS を実施し改善するための原動力であり，適用される法律の遵守と継続的改善に対する最高経営層の約束を反映させることになる。そのために，組織の経営者は所定の間隔で EMS を見直し，評価することになる。しかし，「環境方針」，「経営層による見直し」いずれの項目もがISO9001に比較して，行動規範としての積極性に欠けていると思われる。

4 BS 7799

ISO9000 や ISO14000 は，英国の British Standard Institute が制定した英国国内規格 BS5750, BS7750 が，国際規格に移行したものである[7]。また，安全マネジメントシステムは BS8800 として 1996 年に制定され，ISO ではこれをベースに，ISO18000 OHSMS（Occupational Health and Safety Management System）として国際規格化を検討中であり，現在ドラフトにまでこぎつけている。情報セキュリティの分野では，既に BS7799 という英国国内規格がある。1995 年に制定され，1999 年に改訂版が出版された[8]。この規格も同様に ISO により国際標準とされる可能性があると考えられる。BS7799 は，情報セキュリティマネジメントシステムの要求事項を整理したものであり，情報システム及び情報処理施設の開発運用のための情報セキュリティポリシの作成，企業間電子取引における契約作成にあたって参照すべきガイドラインを具体的に提示している。経営がこの規格を参考にしてセキュリティポリシを作成し，情報セキュリティに関する明確な方向性として組織に提示し，それを支持しコミットすることをBS7799は要求している。また，第11章では，いわゆる危機管理対応手法によるビジネス継続性（Business Continuity）プロセスを展開しているが，ISO9000に見られるように経営者としてコミットすべき内容を明確にしているわけではない。

5 まとめ

規範的セキュリティポリシの重要性を指摘し，その策定の方法論として ISO9000, 14000, BS7799 を比較した。規範性という視点からはISO9000が最も完成度が高く，ISO14000は不充分である。またBS7799は，情報システム全般を対象とし，セキュリティ対策を記述的かつ危機管理対応という視点から整理したものである。

参考文献

[1] 杉野隆 セキュリティポリシ策定に関する考察，経営情報学会秋季全国研究大会予稿集，1998.
[2] 杉野隆 セキュリティポリシ策定方法論について，経営情報学会春季全国研究大会予稿集，1999.
[3] Fraser, Barbara, ed., "Site Security Handbook," RFC 2196 (FYI 8), September, 1997.
[4] Information Technology - Security techniques - Evaluation Criteria for IT Security -- Part 1: Introduction and general model, ISO/IEC 15408-1: 1999(E) 1998.
[5] 情報処理振興事業協会セキュリティセンター ISO/IEC15408「情報技術セキュリティ評価基準」のご紹介，1999.
[6] Joseph Cascio, Gayle Woodside, Philip Mitchell, 日本規格協会 EMS 審査登録センター訳 ISO14000 ガイド 新しい国際環境マネジメント規格，日本規格協会，1996.
[7] 矢野友三郎 マネジメントシステム規格の現状と課題，自動車技術，Vol.51, No.12, 1997.
[8] BS 7799-1: 1999 Code of practice for information security management , 1999.