セキュリティマネジメントの組織への定着

－定着のための５つのキーワード－

アブストラクト

１．はじめに

近年、インターネット環境の大容量高速化が進み、社会基盤として定着していく中で、情報のデジタル化によるサイバースペース上の犯罪や情報漏えい事件も増加してきている。

当分科会では､セキュリティマネジメントの規格やセキュリティ対策技術に焦点をあてるのではなく、現場に即した実践レベルでのセキュリティマネジメントの定着手法の提案にチャレンジすることとした。具体的には、セキュリティ対策を実践する企業の経営者・推進者をターゲットとした、セキュリティマネジメントの導入・定着のための成功要因と手法の提言を本研究の目的とすることである。

代表的なセキュリティ規範であるＩＳＭＳ認証基準をセキュリティマネジメントシステムのモデルとして採用。参加各社の実施状況をもとに､各問題点に共通する主たる原因を抽出し､解決策を提示した。

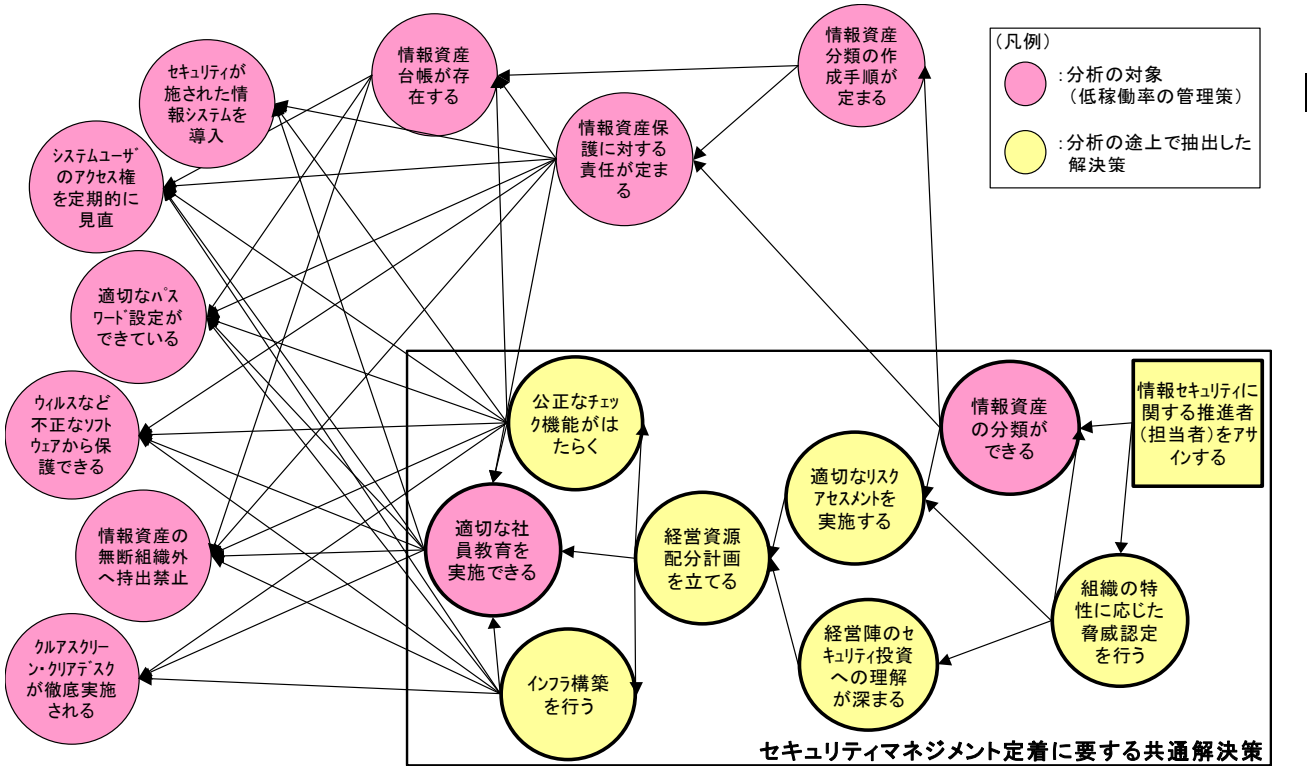
２．セキュリティマネジメントの現状と問題

多くの企業においてセキュリティに対する認識が高まっている。しかしルールの策定のみが目的となっている傾向が散見されており、実際には、実施、監査、改善といったフェーズがうまく実施できていないのが現状ではなかろうか。しかし一般に、なぜセキュリティマネジメントが組織に定着していないのか、原因が明らかにされていないのが現状である。

３．現状分析

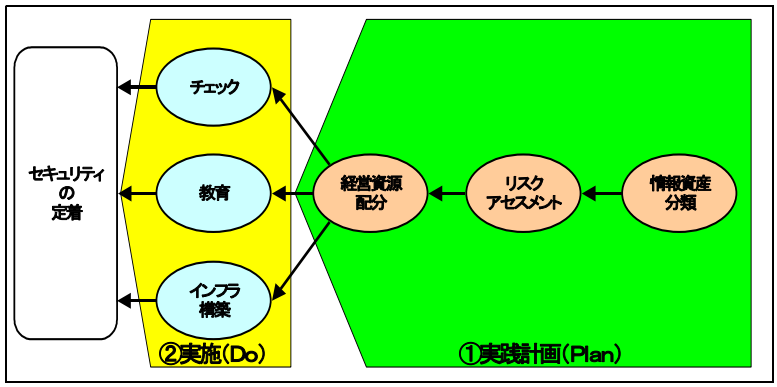
セキュリティマネジメントが定着していない状況について、参加各社を対象に調査を実施した。

調査の結果抽出された「セキュリティマネジメントの組織への定着」を妨げる要因を内包する管理項目を対象に、ＢＲ手法（リザルトチェーン）を用い分析を実施した。（下図）



ＢＲ手法（リザルトチェーン）とは、利益実現プロセスの４つの核となる構成要素（成果、解決策、貢献、前提）の関係を明確にするモデリング技術である。

この分析の結果、セキュリティマネジメントが定着しない原因が、「チェック」「教育」「インフラ構築」「経営資源配分」「リスクアセスメント」「情報資産分類」の６つのセキュリティマネジメント要素の不備によるものであることが判明した。また、各要素の配置より前後関係を分析し、セキュリティマネジメントの定着を達成するための「セキュリティマネジメントのための共通解決策」（右図）を作成した。なお、インフラ構築については当分科会の趣旨に合わないため割愛した。



４．導入定着手法

４．１「情報資産分類」

今日まで組織の情報資産に対しては、「どうやって保護するのか」、その保護方法にのみが着目されてきた。しかし情報資産が多様化している現状においては、組織として「何を保護するのか」を真剣に考えることが重要と考える。情報資産分類の本質は、「所有する財産を把握し、種類毎に分けること」である。原点に立ち戻って、組織が所有する財産（情報資産）を把握すること（考えること）が、本来情報資産分類というプロセスにおいて最初に組織がとるべき行動ではないかと考える。

４．２「リスクアセスメント」

情報資産分類と並んでもう一つ重要なプロセスとして、リスクアセスメントの実施がある。情報資産分類は、リスクアセスメントを実施するうえでの前提条件の一つである。

組織は適切なリスクアセスメントの実施により、セキュリティ上脆弱な部分やそのリスクの大きさについて明確にすることができる。

４．３「経営資源配分」

セキュリティマネジメントを導入し運用するにあたっては、人的・物理的・費用的な資源を必要とする。セキュリティマネジメントの投資においては、情報資産分類とリスクアセスメントを実施しなければ、どこにどれだけの投資をし、どのような効果が上がるかということを見積もることはできない。リスクアセスメントに基づいて経営資源配分計画を立てることが、経営者の責務である。

４．４「セキュリティ教育」

セキュリティ教育については、比較的内容・手法が確立されている「人事・業務系教育」と比較することで、セキュリティ教育の課題を分析した。その結果、セキュリティ教育の目的・必要とされる情報・スキルは対象者の立場によって大きく異なっており、ポジション（階層）別の立場に合わせた教育を実施することが重要である。

４．５「チェック」

ＩＳＭＳ認証基準とセキュリティ監査制度を、企業に浸透している日本の会計制度と比較することで「チェック」に関する問題点を分析した。セキュリティの監査制度は、不足している部分が多い状態である。しかし会計制度も、最初から高度に成熟した制度であったわけではない。セキュリティのチェックにおいても、監査制度の不足している点を補いつつ、チェックを「上手く」実施していく必要がある。

５．結論

セキュリティマネジメント定着のための成功要因と手法は、前述の５つの解決策である。また、この解決策の実施順序も重要である（上図参照）。セキュリティマネジメントを定着させるプロセスは、「情報資産分類」から始まり、次に「リスクアセスメント」を実施する。その結果に基づき根拠のある「経営資源の配分」を行い、「チェック」「教育」などの管理策を実践することが肝要である。これまであまり重要視されてこなかった管理策の実施順序は、実はセキュリティマネジメントを定着させるための重要な役割を担っているのである。