情報セキュリティインシデントデータベースに基づく全社的情報セキュリティマネジメントの強化手法の提案と評価

（課程博士・様式７）（Doctoral qualification by coursework,Form 7）

学 位 論 文 要 旨

Abstract of Doctoral Thesis

専　　攻：　情報科学　　氏　名：　堀川 博史

論文題目：　情報セキュリティインシデントデータベースに基づく
全社的情報セキュリティマネジメントの強化手法の提案と評価

論文要旨：

情報セキュリティインシデントや情報セキュリティ事故の対策の一つとして，情報セキュリティマネジメントシステム（Information Security Management System: ISMS）認証の国際規格および日本規格が制定され，組織の情報セキュリティリスク管理に役立っている．しかし，その現状としては，ISMS 認証を取得している組織でも情報セキュリティ事故が減らない事例が見受けられる．ISMS では，情報セキュリティインシデントからの学習が規定されているが，改善が効果的に働いていない組織もある．筆者は，この課題は，情報セキュリティインシデントからの学習の具体的な方法が手順化されていないことが原因だと考える．そこで本論文では，インシデントデータベースの運用，インシデントデータからの年間予想損失額の算出，インシデントと対策のマトリクスを用いた定期的な対策改善案の選定，対策選定の判断材料となる情報の経営陣への提示から成る一連の方法・手順を「デルタ ISMS」モデルとして具現化する．

情報セキュリティマネジメントの強化は，事業部や事業所を越えた全社的な枠組みの中で達成されるべきものである．ISMS では事業部や事業所といった組織の一部で認証を受けることができるのに対して，本論文ではそのような組織の認証範囲を越えた全社的なセキュリティマネジメントを対象とする．本論文で提案する全社的な情報セキュリティマネジメントの改善は，情報セキュリティマネジメントに責任をもつ経営陣等の配下に編成される組織横断型の「情報セキュリティ統括組織」によって担われる形となる．

ISMS 認証はその附属書の中で，情報セキュリティインシデントの報告や記録を求めている．ある部署でインシデントが起きた際には，当該部署（場合により，情報セキュリティインシデント対応チーム）により 1 次対処（発見された不具合の対処）と 2 次処置（不適合の原因を除去するための処置）までは行われることになっている．しかし規格では，2 次処置の結果を学習することは求めていても，その具体的な手引きを与えていない．このため，ISMS 認証取得組織においても，各部署で発生したインシデントのデータを「組織全体のセキュリティ対策の改善」のために活用していくにあたっての方法・手順については整備されていないという状況となっている．

各部署のインシデントから組織全体の対策改善に資する情報を抽出するための仕組みが不在であるという現状から，マネジメントレビューが認証を継続する活動に主眼が置かれがちとなる背景もあり，インシデント報告が形骸化されがちとなる．すなわち，インシデントデータがマネジメントレビューとしてトップマネジメントに報告される場合，処置が

完了しているか否かの状態が提示されるだけで，トップマネジメントが「組織全体のセキュリティ対策の改善」を行うにあたって必要となる判断材料を提供することが達成されていない．この結果，情報セキュリティリスク管理に対するトップマネジメントの認識が向上せず，組織の情報セキュリティマネジメントが情報セキュリティガバナンスと乖離するという深刻な問題も生じている．

この問題に対し，本論文では，情報セキュリティインシデントデータを「組織全体のセキュリティ対策の改善」のために活用していくための具体的な方法・手順を，「デルタ ISMS」モデルとして具現化する．デルタ ISMS のデルタとは，n 巡目の PDCA サイクルと n+1 巡目のサイクルの差分を指す．

情報セキュリティ統括組織は，インシデントの発生からインシデントの記録をインシデントデータベースに保存する．そして，情報セキュリティ統括組織はインシデント発生部署での 2 次処置が終了した時点で，「当該部署で採択された今回の 2 次処置を，仮に全組織に採用した場合の効果」を算出し，インシデントデータベースに保存する．

情報セキュリティ統括組織は，定期的（例えば半年に 1 度）にインシデントデータベースを精査し，当該期間に発生したインシデント群に対する対策候補を俯瞰することによって，全組織として新たに採用すべき対策の候補を選択する．投資対効果の高い対策を候補として選択するために，インシデント原因と対策のマトリクスである「デルタ ISMS 表」を用い，対策の導入コスト，年間損害低減額と安全係数を用いて対策候補の案を複数自動導出し，トップマネジメントが経営戦略に応じて最適な対策を選択できるようにする．

情報セキュリティ統括組織は，マネジメントレビューの際に，デルタ ISMS 表とともに複数の対策候補案を提示する．トップマネジメントは，この情報を判断材料として使い，「組織全体のセキュリティ対策の改善」を達成するために採用する対策を決定する．取締役会等で CISO 等が経営陣にこれらの情報を説明することで，組織の ISMS と情報セキュリティガバナンスを結合し，経営陣の情報セキュリティリスク管理に対する認識を向上していく．これらの一連の方法・手順が「デルタ ISMS」である．

インシデントは発生頻度が高く被害額が比較的低いヒューマンエラーと発生頻度は比較的低いが被害額が高額な外部攻撃や内部犯行に区分される．ヒューマンエラーに対しては，実組織のインシデントデータを遡りで適用し，実担当者から良好なコメントを得た．外部攻撃に対しては，ケーススタディとして想定した組織が標的型攻撃に対してオーストラリア政府が公表した対策集の導入を検討する場合を示す． 更に，デルタ ISMS の提供する情報と情報セキュリティガバナンスのモニタリング項目と比較することで情報セキュリティガバナンスの視点での有効性を示す．

本論文では，デルタ ISMS として，情報セキュリティインシデントからの学習の具体的な方法を手順化した．すなわち本論文は，微視的には，JIS Q 27001:2014 の中の「情報セキュリティインシデント管理（A.16)」に係る一貫性のある効果的な取組みについて手順化するものであり，JIS Q　27001:2014 を補完することを目的とする．一方で，本論文は，巨視的には，全社レベルの情報セキュリティマネジメントの改善に係る一貫性のある効果的な取組みについて手順化するものであり，組織の情報セキュリティガバナンスを補強することを目的とする．