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９）　　審　査　要　旨

専攻　情報科学専攻　学籍番号　５５４４５０３１　学生氏名　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

情報セキュリティ事故の対策の一つとして、ISMS（情報セキュリティマネジメントシステム）認証が制定され、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、現状としては、ISMS 認証を取得している組織でも事故が減らない事例が見受けられる。計画段階においては運用段階で発生する情報事故をすべて想定しきることはできないため、ISMS においては、その定常的な改善が必須となるが、その具体的手順が確立されていないという大きな課題が残っていた。

そこで本研究では，運用段階において自組織内で発生した事故情報をデータベースに蓄え、その分析から対策の改善案を選定するとともに、経営陣と協調して実際の改善策を決定するための一連の方法・手順を「デルタ ISMS」手法として定式化する。これにより各組織は、ISMS の PDCA（Plan-Do-Check-Act）サイクルを継続的に回すことが可能となる。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。

第 1 章は序論であり、本研究の背景、現在の ISMS における課題について述べている。

第 2 章では、関連する既存研究や調査を通じて現在の ISMS の課題を分析し、本研究が解決すべき要件を明確化している。

第 3 章では、デルタ ISMS 手法の具体的な手順を説明している。「事故データベース」の運用と管理によって、事故発生部署における対応を全社レベルに引き継ぐ。「デルタ ISMS 表」の作成によって、複数の対策候補の中から当該事故に対して最善な（費用対効果の高い）対策の選択を可能にする。「安全係数」の導入によって、安全性を重視した際の対策と経済性を重視した対策を選出し、経営陣の判断を導く。

第 4 章では、本研究にて提案したデルタ ISMS 手法を、実組織の過去の情報事故の事例、ならびに、仮想組織に対する標的型攻撃被害の事例に対して適用することによって、提案手法の有効性を実証している。また、情報セキュリティガバナンス導入ガイダンスのモニタリング項目との比較を通じて、提案方式が全社的な管理改善方法として適格であることを示している。

第 5 章では、本研究をまとめると共に、本研究の研究成果を活かした今後の展望について述べている。

以上のように、本論文は、情報システムの安全な管理運用を具現化するための具体的な方法・手順を定式化するとともに、その有効性を実証しており、実効的な ISMS の確立に寄与するところが大きい。本論文は当該分野において多大なる価値を持ち、その社会的貢献に関するポテンシャルも高い。よって、本論文は博士（情報学）の学位を授与するのに十分な内容を有するものと認める。