博士請求論文審査要旨

情報セキュリティ大学院大学
情報セキュリティ研究科

論文題目　：　組織の情報セキュリティリスク対応を支援するモデルの提案とその適用可能性の検討
―ISO/IEC 27001:2013 及び ISO/IEC 27002:2013 適合モデルとその運用手法について―

申請者　：　川﨑 律子

審査委員会　：　主査　教授　廣松 毅
副査　教授　田中 英彦
副査　教授　佐藤 直
副査　教授　原田 要之助

Ⅰ. 論文内容の要旨

本論文の目的は、情報セキュリティリスクマネジメントのうち、特に情報セキュリティリスク対応を支援するモデルを提案することによって、情報セキュリティリスク対応に伴う組織における意思決定を支援することである。

本論文は全 6 章から構成されており、各章の概要は次の通りである。

1 章の序章では、研究の背景と研究目的および先行研究のまとめを述べている。

2 章では、本論文が提案しているモデルの概要、およびモデルを構成する要素について説明している。構成要素のうち、情報セキュリティリスクのリスト、各情報セキュリティリスクのリスク値、リスクヘッジ策のリスト（これらの設定は ISO/IEC 27001:2013 及び ISO/IEC 27002:2013 に基づいている）、各リスクヘッジ策実施に必要な費用、さらに各リスクヘッジ策の各情報セキュリティリスクに対する影響値は、モデルにおいては固定値として扱うとしている。

3 章では、サンプルデータを用いたモデルの基本動作の確認とモデルの活用方法について記している。提案モデルを活用することで、与えられたリスク受容値に対する組織の予算の最小値の導出および与えられた組織の予算に対する最小リスク受容値の導出が行うことができることを示している。

4 章では、統計データを用いて提案モデルの適用可能性について検証を行っている。本モデルが必要とする要素は、一般にはセキュリティ上の理由から公表されていないため、ここでは、公表されているデータとして、経済産業省による平成 25 年度版情報処理実態調査の結果を用いている。

5章では、実在する組織において実施された情報セキュリティリスクマネジメントのデータを用いて提案モデルの有効性を確認している。データは、ある組織(A社としている)の1部門が、ISMS認証取得をめざした際に実施した情報セキュリティリスクマネジメントに関するものであり、そこからリスクの一覧、各リスク値、各リスクヘッジ策実施にかかる費用、各リスクヘッジ策の各リスクに対する影響値、リスクヘッジ策実装に対する組織の予算、リスク受容値に関する情報を得て、提案モデルで使用できる内容に修正している。モデルによる解は、A社が実際に対策を選択結果とは異なる内容となったものの、本論文では、その理由を示し、またモデルによる解が、A社にとって妥当な内容であることを確認している。つまり、モデル適用により選択されたリスクヘッジ策は、A社の状況に沿った内容であること示している。

なお、この章で用いられているデータは特定の組織の秘密に属する情報が含まれているため、社名を伏せる

ほか、原資料の信頼性等については委員会が in camera 方式で確認をした。

最後に、第６章は、本論文の結論として得られた結果と今後の課題を述べている。

また付録としてＡ：影響値の算出方法、Ｂ：基本モデルの汎用表計算ソフト上での実装及び各種設定、Ｃ：リスクヘッジ策と ISO/IEC27002:2005(JIS Q 27002:2006)管理策との対照表を付けている。

Ⅱ. 論文審査結果の要旨

本論文は、組織の情報セキュリティリスクマネジメントのうちの情報セキュリティリスク対応を支援するモデルの構築とモデルに必要な要素の摘出・設定（2 章）およびモデルの適用可能性と有効性の検証（3～5 章）からなる。それぞれの部分において、抽象的になりすぎず、複雑すぎない実践的な内容にするように努力をしており、経営者が組織の情報セキュリティに関わるリスク全般を把握した上で、組織の予算制約のもとでどのリスクにどの程度の費用を配分すれば、どの程度情報セキュリティレベルが達成できるかに関する意思決定を支援するものとなっている。特にモデルの有効性を検討するにあたって、実際の企業のデータを用いて検証を行っている点は特筆すべきであり、本論文の最大の特徴である。ただし、モデルの単純化のために、リスクヘッジ策の実装にかかる費用はかなり限定された条件のもとで算出されていること、またリスクヘッジ策の選択割合と実装費用については単純に正比例するとしている点などについては、より実態に近い内容を反映するために改善が必要であり、今後の研究の発展を期待したい。

以上の諸点を総合して、本論文は組織の情報セキュリティリスクマネジメントの発展に大きく貢献するものであり、博士（情報学）の論文として合格と認められる。

Ⅲ. 審査経過

本審査委員会は、27 年 1 月 28 日に論文内容とこれに関連する事項について口述試問を行い、申請者が学位取得にふさわしい知見を持つものと判断した。