# 論 文 の 内 容 の 要 旨

論文題目　　情報セキュリティマネジメントのモデル構築に関する研究

氏　名　　川中　孝章

本研究は、情報セキュリティマネジメントの問題に対して、事象をモデルするアプローチにより、その構造解明を行い、問題解決のための知見を導くことを目的としている。

情報化社会が進展するに伴い、インターネットやパソコン、携帯端末などの普及により、人々が情報共有しやすい仕組みが整った反面、情報セキュリティの問題が浮上してきた。コンパクトなメモリーに大量の情報を記憶でき、多くの人々とたやすく、迅速に情報共有できるようになると、逆に、共有したくない、あるいは、されるべきではない情報も共有してしまうという事態が起こってくる。その意味で、情報共有と情報セキュリティの問題は表裏一体の関係にあるといえる。情報化社会の負の側面であるこの問題は、技術面、経営面、法律・制度面、倫理面などの、幅広い分野にまたがる問題領域を有している。

本研究では、この問題に対して特に経営面からアプローチを行い、

① 情報セキュリティの脅威-脆弱性-対策に関する概念モデル（第 2 章）
② マルチエージェントによる情報セキュリティの脅威-脆弱性モデル（第 3 章）
③ 情報セキュリティの脅威-脆弱性-対策に関する構造分析モデル（第 4 章）
④ クラウドサービス市場における情報セキュリティ監査モデル（第 5 章）
⑤ 情報セキュリティにおける「ペイル・マネジメント」の概念モデル（第 6 章）

といった、情報セキュリティの問題を多面的に検討するためのモデル構築を行い、その分析結果を提示する。

第 1 章では、研究目的、問題領域、基本概念の定義、前提条件と限界、先行研究と本研究の特徴について記述し、本研究の対象や位置づけを明らかにする。これにより、研究の基礎となる概念を明らかにし、第 2 章以降の議論の基礎固めを行う。

第 2 章では、本研究全体を通じての基本モデルとなる「情報セキュリティの脅威-脆弱性-対策に関する概念モデル」を提案する。これは、情報セキュリティにおけるリスク分析の構成要素である、情報資産、脅威、脆弱性の三つの要素に、情報セキュリティマネジメントの中核である情報セキュリティ対策を加えて、それらの関係性を記述したものである。従来のリスク分析では、情報資産、脅威、脆弱性の定量化に重きを置いている反面、マネジメントにおいて重要となる情報セキュリティ対策との関係については、あまり触れられてこなかった。リスク分析の長所をマネジメントの研究に生かすために

は、対策を含めた構成要素間の関係を明確にすることが必要であり、本研究の提案モデルは、これを含めた情報セキュリティ事象全体を表す概念モデルとなっている。その上で、脅威は対策によって制御できず、脆弱性は対策によって制御できるものとの考え方を提示し、不確実性が大きいものとそうでないものを明確にしている。

第 3 章では、第 2 章のモデルを基礎として、脅威と脆弱性の関係をマルチエージェントによりモデル化し、シミュレーションによって情報セキュリティマネジメントの問題解決を図るための方法を提案する。これは、情報資産エージェントと脅威エージェントにそれぞれ脆弱性と脅威を表す属性を持たせ、コンピュータ画面上に作成した仮想の企業平面内に、両エージェントの攻防による情報セキュリティ事故を再現できるようにしたものであり、事故を確率的に発生させ、属性の値を変化させることによって事故発生の状況がどのように変化するのかを測定できるようにしている。そして、この方法が、実際の企業では測定することが難しいとされる情報セキュリティ対策と結果の関係を、研究者の意図する環境条件の下で繰り返しシミュレーションにより測定できる方法であることを示すとともに、情報セキュリティマネジメントの定量的研究手法として有効なアプローチであることを提案する。本研究ではその一例として、情報セキュリティマネジメントがボトムアップで行われるべきか、トップダウンで行われるべきかについてシミュレーションを行い、ボトムアップ方式が局所最適に陥りやすく、トップダウン方式がより情報セキュリティマネジメント上の全体最適を実現しやすいという示唆を導いている。

第 4 章では、第 2 章の概念モデルと、第 3 章のシミュレーションモデルを基礎にして、情報資産を取り巻く、脅威、脆弱性、対策の関係を数理モデルにより記述し、さらにそのモデルに大規模な実証データを適用することにより、情報セキュリティ事象全体の構造解明を行う。第 3 章では情報セキュリティ事故が脅威と脆弱性の関係から確率的に起こることを基礎として、エージェントによるモデル化を行ったが、第 4 章では、対策の実施が事故の発生件数に直接的に影響を及ぼすのではなく、一旦情報資産の脆弱性を改善し、それが事故の発生に影響を与えるという仮説を立てる。そして、それを検証するために回帰モデルをあてはめ、因果関係を測定する。情報セキュリティ事象について、仮説、検証のアプローチにより、その構造解明を行うものである。これにより、この事象が決定論的事象と確率論的事象の二重構造により成り立っていることを明らかにし、対策によって制御できる部分とそうでない部分に区分できることを提案する。その上で、事故はなくならないものであるとの認識の下、事故が起こる前の予防措置と起こった後の回復措置の両方への備えが必要であること指摘する。現在、事故が起きていないからといっても、やるべき対策を怠っていれば、それはたまたま事故が起きていないだけであり、脆弱性を放置していると事故の発生確率は大きいまま、いつ事故が起こってもおかしくない状態が続くことを、この二重構造は物語っている。

第 5 章では、第 4 章の分析によって得られた情報セキュリティ事象の構造に関する知

見を元に、情報セキュリティ監査制度についてゲーム理論的観点から考察を行う。例として今後その発展が予想されるクラウドサービス市場を取り上げ、その健全な発展のために情報セキュリティ監査が果たすべき役割について述べる。さらに、この監査制度が市場において信頼され、制度として有効に働くために、監査報酬、監査品質、情報セキュリティ対策の不確実性などが、どのような条件を満たすべきであるのかについて提案する。具体的には、クラウド事業者とクラウド利用者の間にセキュリティ面での情報の非対称性があることに着目し、それを解消するための制度として情報セキュリティ監査制度があることを指摘する。また、類似した監査制度である会計監査制度のモデルと比較しながら、両者共通の問題点、情報セキュリティ分野特有の問題点など、様々な問題の解決のためにモデルにパラメータを与え、その値を変化させながら理想の監査制度を探求するというアプローチを試みる。これにより、監査報酬をクラウド利用者が監査人に支払うケースが監査人の独立性を高める反面、その場合において監査制度が市場から信頼を得るには、監査人による高い精度の監査とクラウド事業者による効果的な情報セキュリティ対策が求められるということがわかった。

第 6 章では、組織の情報セキュリティレベルを改善していくためには、どのようなコンセプトの下にマネジメントを行えばよいのかについて提案を行う。組織の情報セキュリティレベルを向上させるためには、多くのメンバーが協力して対策を実践していかなければならない。個々の問題毎の局所最適に陥ることなく全体最適を実現するには、組織全体を見わたせるマネジメントシステムの導入が必要である。情報セキュリティは桶にたとえられることがあるが、従来のこの考え方に加えて桶の箍（たが）の役割も重要である。桶の水面の高さを組織のセキュリティレベルの高さとすると、桶の側板を伸ばすことに加えて箍を締めることが水面（セキュリティレベル）を高く保つ秘訣である。側板を伸ばすことは個々の領域での対策活動を表し、箍を締めることはナレッジチェーン・マネジメントと PDCA（Plan→Do→Check→Act）による継続的改善活動を表す。このマネジメント・コンセプトは、組織内で情報セキュリティ対策活動に取り組むメンバーの職務満足と企業の社会的信用の向上を同時に達成しようとするものである。

第 7 章は結論であり、本研究の議論を整理するとともに、各章の提案モデルや考察から得られた研究成果を明らかにする。これにより、情報セキュリティマネジメント研究の新たな方向性を示唆するとともに、本研究の限界を踏まえた上での今後の研究課題について整理する。

これまでの情報セキュリティマネジメントの定量的研究は、リスク分析の観点からの対策選定手法の開発や、対策を行う人の心理的研究などが主であり、組織を舞台としたマネジメントの研究というよりも、個々の手法の開発や人そのものに焦点をあてたミクロ的な研究が中心であった。これに対して本研究は、企業の経営者の立場から見て、情報セキュリティマネジメントをいかに行うべきかという点に焦点を当てている。この視点に立ち、これまで着目されてこなかった「情報セキュリティマネジメントの実験環境

を構築し、それにより対策の効果を測定する方法」を提案し、「大規模な実証データによって情報セキュリティ事象の構造解明を行い、マネジメント上の知見を獲得」するとともに、さらに、今後発展が予想されるクラウドサービス市場を例として、「情報セキュリティ監査が制度としてうまく機能するための条件を導く方法」を提案した。これが本研究の主たる貢献である。