

# A Study on Evaluation Methodology of Cybersecurity Investment

石川, 朝久

<https://doi.org/10.15017/1928635>

---

出版情報 : 九州大学, 2017, 博士 (工学), 課程博士  
バージョン :  
権利関係 :

氏 名 : 石川 朝久

論 文 名 : A Study on Evaluation Methodology of Cybersecurity Investment  
(サイバーセキュリティ投資評価手法に関する研究)

区 分 : 甲

## 論 文 内 容 の 要 旨

サイバーセキュリティ事故は毎日のように発生しており、サイバーセキュリティは IT の問題ではなく、経営マネジメントの問題と認識され、対策の推進が重要とされる。セキュリティ対策は、ガイドライン・規制を参考に適切に実装すれば、その多くを予防可能である。しかし、セキュリティ対策をどこまで実施すればよいか投資基準は明らかでなく、セキュリティ戦略上の課題である。

セキュリティ投資の妥当性を検証するため、モデル・過去事例を通して妥当な想定被害額の算出が重要となる。調査費用や顧客対応費用など「有形コスト」(Tangible Cost)のみならず、企業価値・ブランディング低下など「無形コスト」(Intangible Cost)についても検討が必要である。本論文では、セキュリティ投資評価手法に関して次の重要な3つの課題を研究した。

第一に、個人情報漏洩時の賠償価格について、理論モデルの算出価格と実際に訴訟・自主的な「お詫び」を通じて支払われる金額に乖離がある。2003年に「JOモデル」が定式化され、個人情報漏洩時の賠償価格を算出するベンチマークが提案された。この背景には、2002年に関する個人情報漏洩の賠償金の判例が出たこと、2003年に個人情報保護法が制定されたこと、事故情報の開示件数が非常に少ないことが挙げられ、現在でも利用されている。一方、2003年の情報セキュリティ事故を前例に、事故発生時には500円の金券を送付することが慣習化された。

第二に、セキュリティ事故発生時における企業価値への影響を評価する手法として、株価の時系列情報を利用したイベント・スタディ手法が知られているが、株価を持たない企業には応用ができないという課題が存在する。この既存手法は、「株価が企業価値を示す指標である」という前提の下、イベント前後の株価の変動に注目して「累積異常変化率」を算出し、イベントが株価にもたらす短期的影響を分析する方法である。しかし、非上場企業などに応用できないため、既存手法の応用範囲の観点から改善が必要となる。

第三に、「サイバー保険」について、投資の有効性分析が十分に行われていない。保険は代表的なリスク転移手法であるが、サイバー保険の制度設計・導入の黎明期であるため、伝統的な保険数理手法が使えず、有効性・費用対効果について様々な意見・議論がある。しかし、変動性の高い費用を固定化する「サイバー保険」は、今後より重要になると推測される。様々な条件を入力して評価を実施できる手法を採用し、現時点での有効性を示す必要がある。

本学位論文は以下のように構成される。

第1章では、本研究の背景と目的を述べる。また、本研究の主要な課題と貢献についても論じる。

第2章では、セキュリティ投資評価手法と被害額推定手法に関する背景知識と既存手法について説明する。既存研究を体系的に整理することで、上記で挙げた研究課題を抽出した。

第3章では、第一に日本における個人情報漏洩事件 45 件の事例分析を行い、企業が金券・商品券を送付した平均金額が 543 円であり、JO モデルの理論値と 60 倍以上の差異があることを示した。第二に、米国と日本における訴訟について事例分析を行った。日本では賠償金額が 1 名当たり平均 5,000 円以上である一方、米国では平均 1 ドル以下であることを突き止め、日本の賠償金額が平均的に高いこと、および賠償に対する考え方の違いを論じた。第三に、個人情報の取り扱われ方の変化について検討を行い、モデルが改善すべき点について「検索容易性」、「変更容易性」、「回収容易性」という 3 つの特徴を指摘した。

第4章では、株価の代替として、「ツイート感情指数」を定義し、インシデントによる企業価値への影響を測定する手法を提案した。「ツイート感情指数」とは、調査対象企業のツイートに対して感情分析を行い、数値化されたデータを単位時間毎に累積した値である。この「ツイート感情指数」の時系列情報に対して、イベント・スタディ手法を適用し「累積異常変化率」を算出することにより、インシデントの影響を分析する。事例分析では以下の結果を得た。第一に、上場企業の株価・「ツイート感情指数」の両時系列情報に対してイベント・スタディを実施し、短期間（イベント日前後 1 日を含む計 3 日間）の範囲で、両時系列情報に相関係数 0.8 以上の強い相関性があり、「ツイート感情指数」が株価の代替として利用可能であることを示した。第二に、非上場企業の事例について考察を行い、企業価値の影響を測定できることを示した。

第5章では、第一にサイバー保険の仕組み・現状・課題について、技術的・経済学的の観点から分析を実施した。その後、具体的な想定事例を元に、定量的な費用便益分析を実施した。情報漏洩の発生確率や漏洩件数など想定シナリオにより結果が変化するため、モンテカルロ・シミュレーションを利用して考察を行った。被害コストの公開事例に基づく仮想企業の事例では、投資対効果は約 200 倍、保険の被害額カバー率は約 65%という結果となり、サイバー保険が被害額を抑え、有効性があるという結論を得た。

第6章では本研究の結論を述べ、今後の研究課題について論じる。