

企業の情報セキュリティ事故による株価への 影響に関する実証研究

Empirical Study on the Impact of Stock Price by Corporate Information Security Incidents

田中 勝行¹
Katsuyuki Tanaka

(論文要旨)

本研究の目的は、企業が起こした情報セキュリティ事故の公表が株価へ与える影響を検証することである。「日本における情報セキュリティ事故の公表は、企業の株価に負の影響を与える」、「情報セキュリティ事故の公表は、IT 企業の事故の方がその他の業種タイプの企業の事故より、企業の株価により大きな負の影響を与える」、「情報セキュリティ事故の公表は、ISMS 認証取得企業の事故の方が未取得の企業の事故より、企業の株価により大きな負の影響を与える」という3つの仮説を立て、イベントスタディ手法を用いて公表された163件の情報セキュリティ事故を統計的に分析した。その結果、情報セキュリティ事故の公表は企業の株価に負の影響を与えること、IT 企業の方が影響が大きいこと、さらにISMS 認証取得企業の方が影響が大きいことが明らかになった。

1 はじめに

情報通信技術(Information and Communication Technology. 以下、ICT)が進歩し生活が便利になる一方で、情報漏えい、情報改ざん、コンピュータウイルスの感染、システムのサービス停止など、情報セキュリティ事故は毎日のように発生している。企業は事故を起こしてしまうと、顧客に対する損害賠償や自社内での原因調査や再発防止のためにコストが発生し、さらには信頼の失墜につながる。ICT が進化するに従い、事故も高度化、多様化してきており、情報セキュリティ対策は一時的な対策ではなく、維持し改善していかなければならない。一方、対策が重要であると認識されているが、リーマンショック以降の経済不況で ICT 投資への抑制が強まる中、情報セキュリティ関連の投資を減少させる企業が増えているⁱ。情報セキュリティは、その技術的な難解さなどのため経営者から見た場合、投資の判断が非常に困難になる場面も少なくない。情報セキュリティ事故のようなオペレーショナルリスクやレピュテーションリスクは一度顕在化すると多額の損害を与える

¹ 青山学院大学 国際マネジメント研究科

反面、リスクが顕在化しにくいため、経営者は情報セキュリティに対して投資を行うインセンティブが働きづらい側面がある。また情報セキュリティ対策に多様化のため事故防止の投資効果の評価が難しく、情報セキュリティ投資に消極的な態度を取っている経営者が多い。

著者が企業の情報セキュリティ投資がセキュリティ向上に及ぼす影響を、経済産業省が実施した平成 21 年度情報処理実態調査の個票データを統計的に分析した結果ⁱⁱ、情報セキュリティ対策は技術的な対策よりも従業員への情報セキュリティ教育、セキュリティポリシーの策定、内部統制の整備強化などの組織的対策が情報セキュリティ事故を防止する効果に有効であることを明らかにした。

一方、情報セキュリティ事故が企業に与える影響を企業に対する想定損害賠償総額ⁱⁱⁱで量的に表したのが、図 1 である。2007 年度は漏えい人数が極めて多い、大きな情報漏えい事故が 2 件発生したため、想定損害賠償総額が高額となっているが、それを除いてもこの数年間の想定損害賠償総額は 1000 億円から 5000 億円となっている。情報セキュリティ事故一件あたりの想定損害賠償額の推移を図 2 に示した。これによるとこの数年の一件あたりの想定損害賠償額は 7500 万円から 5 億円である。この図が示していることから情報セキュリティ事故の発生及びその事故の公表が、企業価値に影響を与えているのではないかと考えられる。

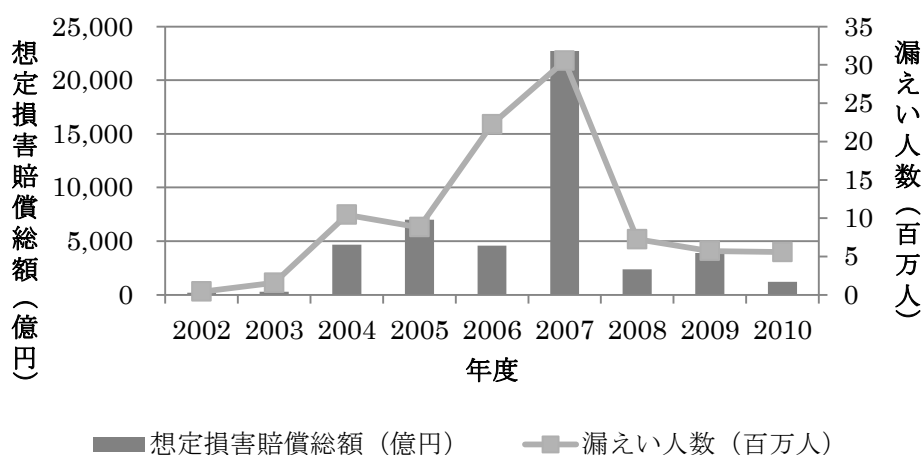


図 1 情報漏えい人数と想定損害賠償総額の推移^{iv}

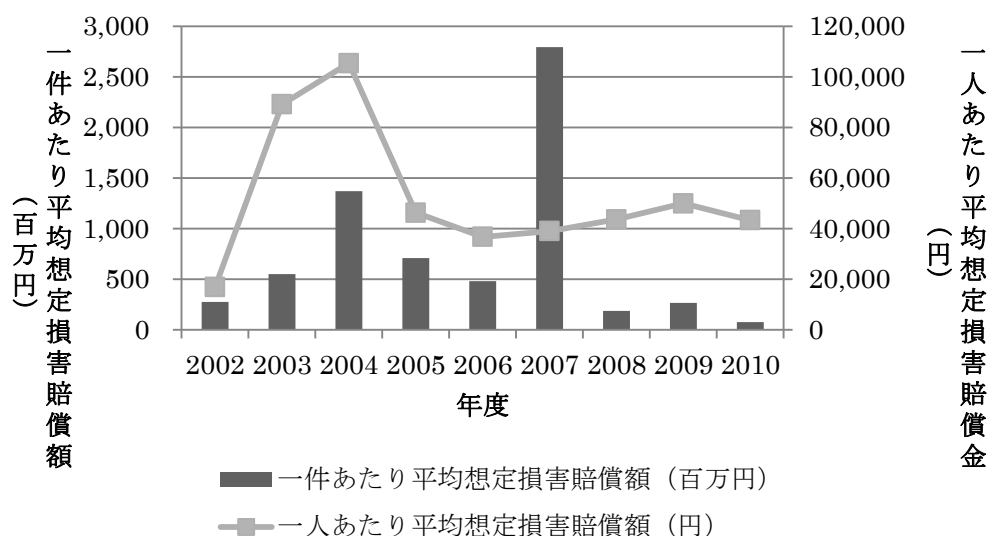


図 2 一件あたりの平均想定損害賠償額と一人当たり平均想定損害賠償金の推移^{vi}

実際、2011 年 4 月に発生したソニー株式会社の個人情報漏えい事故では 7700 万人分の情報が流出し、事故公表の翌日にはソニー株が 4 % 下落した。仮に一人当たり 1,000 円の補償額として、800 億円近くのコストが発生する。また顧客に多額の賠償金の支払いを迫られるとの懸念もあり、投資家が持ち株を縮小したことにより、株価が下落した。

企業価値をどのように定義するか、企業価値をどのように計測するかは本研究の重要なテーマのひとつであるが、本研究では定量的に判断が可能である株価を用いて検証を行った。株価はある時点の企業に関するあらゆる公式な情報によって決まるので、企業価値を数値的に評価できる最良の指標であると考えた。企業の情報セキュリティ事故が当該企業の株価に及ぼす影響を検証することができれば、企業の経営者が情報セキュリティへの投資判断する際の合理的な意思決定の判断材料のひとつとして、利用することに貢献できると考える。

以上のように、企業の情報セキュリティ事故が企業価値、すなわち株価に与えている影響について、公表されているデータから検証することが本研究の目的である。

本研究の構成としては、第 2 章で本研究と関連性が高い先行研究について述べ、そこでの議論から仮説を構築する。第 3 章では、実際の収益率のデータを使って株価への影響について検証を行う。最後に第 4 章では本研究のまとめと今後の課題について述べる。

2 先行研究と仮説

2.1 先行研究

本研究分野では、企業の情報セキュリティと企業価値との関係に着目したいいくつかの研究がある。情報セキュリティ投資は、株価に不利に影響する悪意あるセキュリティ攻撃を減らす効果があること、さらに情報セキュリティ製品やサービスに対する高い要求が情

報セキュリティ対策に肯定的な見方として伝えられ、企業の株価の増加と関連していることが報告されている(Khansa and Liginlal, 2009). また不正アクセスや機密情報の流出などの脅威の増加が、情報セキュリティの取り組みを企業のITマネジメントの中核と位置づけるようになってきている(Dutta and McCrohan, 2002). 実際、グローバル組織の90%が情報セキュリティは事業を成功させるのに非常に重要であると考えている(Ernst, 2003). 一般に情報セキュリティ対策の目的は事業を継続することを保証することであり、さらには評判やブランドイメージを守ることである(Nash, 2008). 企業がネットワークを強化することや、ウェブサイトをセキュアにするために情報セキュリティに予算を継続的に増加させているが、情報セキュリティマネジメントに対する最も大きな障害は不十分な予算である(Ernst, 2008). 2003年に行われたグローバルなセキュリティ調査では、平均して企業は情報セキュリティ対策にIT予算の6%しか使っていない(Ernst, 2003). また情報セキュリティに十分な財源を得ることの主な障害は情報セキュリティ投資に対するリターンを正当化することが困難なことである(Cavusoglu et al., 2004). 予防技術および情報セキュリティ投資の最大の効果は「悪いことが何も起きないこと」である. よって内的または外的な要因によるウイルス攻撃やセキュリティ侵害などのセキュリティ事故の本当のコストを解明することは効果的なセキュリティマネジメントの戦略および方針を作成するのと同様に重要なことである.

しかしながら、セキュリティ事故のコストの評価は多くの企業ではしばしば無視されている. それは情報セキュリティ投資のコストと利益構造を定量化することの困難さが理由の一つである. この困難さの主な原因は経済的、財務的な分析のための正確な評価指標や効果的な手法がないことによるところが大きい. さらに分析を複雑にさせている理由は、セキュリティ事故が有形と無形の両方のコストに影響を与えているからである(Mercuri, 2003).

コンピュータウイルスやセキュリティ事故の目に見えるコストについて、多くの報道やレポートがあるが、これらの数字のほとんどは、正確性や信頼性の点で問題がある. その理由のひとつはセキュリティ事故自身を検出することや、たとえばコンピュータ攻撃を検出することが実際に攻撃されている数より少ないことによる. また検出された攻撃やコンピュータ侵害の検出のすべての事故が報告されているとは考えられないからである. 情報漏えい事故のために、どのくらい顧客の信頼やロイヤリティを失ったかという目に見えないコストを算出することは極めて困難である. 加えて、当該企業のその後の法的なコスト、たとえば損害賠償額などを事前に見積もることもほとんど不可能である.

このようにセキュリティ事故の本当のコストを見積もることは非常に難しいので、直接的なコストを見積もる代わりに代替の手段を用いる研究がされている. Ohlsonモデル式(Ohlson, 2001)を基にして、情報セキュリティに関する事故の自発的公表の市場価値を統計的に分析している(Gordon et al., 2010). Ohlsonモデル式は企業の株価を、貸借対照表の純資産額および損益計算書の当期純利益を用いて表現しているが、それに情報セキュリティ

事故の公表の有無などの要素を追加して分析している。その結果、情報セキュリティに関する事故の自発的公表は当該企業の市場価値に影響を与えることを示している(Gordon et al., 2010)。

また最近では、情報セキュリティ事故の潜在的なコストの代替手段として、イベントスタディの手法を用いて当該企業の株価に対するセキュリティ事故の影響を見積る研究がされている。株価はある時点の企業に関するすべての公式な情報によって決まる企業価値に反映されると仮定できるので、特定の事故による株価の変動は、市場操作を受ける会計情報を基にした測定より効果的に、事故の財務的な影響を図ることができる(McWilliams and Siegel, 1997)。イベントスタディの手法は、会計、財務、マネジメントなどの分野で応用されている。IT関連では、IT投資の影響を企業の市場価値で測る研究がある(Dehning et al., 2003)。また、Eコマースの発表の影響(Subramani and Walden, 2001)、Webトラフィックの発表の影響(Benbunan-Fich and Fich, 2004)をイベントスタディで分析している研究がある。イベントスタディの手法を使用して、セキュリティ侵害が公表された後に、当該企業の企業価値に影響を与えるか否かを、累積超過収益率(CAR: cumulative abnormal return)を用いた実証研究が行われている。1995年から2000年までの米国企業を対象に、情報セキュリティ侵害の中でも機密性の高い情報の場合には、企業価値がネガティブに反応することが確認されている(Campbell et al., 2003)。また1996年から2001年までの米国企業を対象に、侵害の種別、企業の規模、業種について分析した結果、情報セキュリティ侵害によって、2.1%の企業価値が損なわれ、企業規模が小さくなるほど損害幅が大きくなると報告されている(Cavusoglu et al., 2004)。さらに情報セキュリティに関連したイベントに対する株式市場の反応を、情報セキュリティ侵害の要因、ビジネスの種別、産業、侵害の種別、発生した年、イベントウインドの長さなどの効果を考慮した研究がある(Yayla and Hu, 2011)。この研究では最近のEコマース企業は古くからある伝統的な会社よりも大きなネガティブな株価の反応を示すことを明らかにしている。日本での研究では情報セキュリティ投資と企業価値をイベントスタディの手法を用いて研究したものがある(高籾 et al., 2010)。この研究では企業の情報セキュリティ投資が市場にアナウンスされると株価が上昇すること、またクレジットカード情報の漏えい事故が企業価値に負の影響を与えると述べている。

情報セキュリティ事故による影響をイベントスタディの手法を用いた先行研究を表1のようにまとめることができる。イベントスタディによる情報セキュリティ事故による企業価値への影響を研究した先行研究では、情報セキュリティ事故の種類を限定した研究が多い。たとえばDos攻撃のみを対象とした研究(Hovav and D'Arcy, 2003)、(Ettredge and Richardson, 2003)、(Garg et al., 2003)、ウイルス攻撃のみを対象とした研究(Hovav and D'Arcy, 2004)、クレジットカード情報の漏えい事故を対象とした研究(高籾 et al., 2010)などである。これらの研究では表2のような種類の情報セキュリティ事故の公表が株価に影響を与えているかを分析している。一方、Yayla and Hu(2011)は、情報セキュリティ事故の

種別間での影響の違い、さらに年代や E コマース企業と非 E コマース企業との比較を分析している。DoS 攻撃を受けた企業の株価は有意に影響を受けているが、それ以外の事故の場合は影響がない。

また 2000 年以前の事故の公表は株価に影響を与えているが、2000 年以降の事故の公表は株価に影響を与えていない。さらに E コマース企業は情報セキュリティ事故の公表が株価に有意に影響を与えているが、非 E コマース企業では影響はないと報告されている(Yayla and Hu, 2011)。

本研究では情報セキュリティ事故の種別に注目するのではなく、事故を公表した企業の特徴に着目し、どのような企業が情報セキュリティ事故を公表した場合、株価への影響が大きいかを分析する。

表 1 イベントスタディによる情報セキュリティ事故の企業価値への影響に関する研究

Author	Sample Size	Sample Period	Events Windows	Results
Campbell et al.(2003)	43	1995-2000	[-1,1]	全サンプルと非機密情報の事故に対しては不十分なネガティブな反応 機密情報に対する事故に対しては十分にネガティブな反応
Hovav and D'Arcy(2003)	20	1998-2002	[-1,0] [-1,1] [-1,5] [-1,10] [-1,25]	全サンプルに対して不十分なネガティブな反応。Dos攻撃のみを対象。
Ettredge and Richardson(2003)	4	2000	[0,0] [0,1] [0,2]	十分なネガティブな反応 ただし、調査した対象は2000年2月に発生したDoS攻撃のみを対象。
Garg et al.(2003)	22	1999-2002	[0,0] [0,1] [0,2]	全サンプルに対して十分なネガティブな反応 Different effect sizes among type of security breaches 以下の4つのタイプ (1) DoS, (2)クレジットカード情報の流出, (3)顧客情報の流出, (4)Webサイトの改竄
Hovav and D Arcy (2004)	186	1988-2002	[0,0] [0,1] [0,5] [0,10] [0,20]	全サンプルに対して不十分なネガティブな反応 ウイルス攻撃のみを対象。
Cavusoglu et al.(2004a)	66	1996-2001	[0,0] [0,1]	全サンプルに対して十分なネガティブな反応 ビジネスタイプ、企業規模、イベントの期間 セキュリティ事故のタイプに対しては不十分なネガティブ。タイプとしては (1)DoS, (2)その他。
高藪 他(2010)	10	2004-2008	[-10,10]	クレジットカード情報の漏えい事故に関してネガティブな反応
Yayla and Hu(2011)	123	1994-2006	[-1,1] [-1,5] [-1,10]	E-コマース企業はその他の企業よりもネガティブな反応 DoS攻撃は他のセキュリティ事故よりもネガティブな反応 近年に発生したセキュリティ事故の方が、インパクトが少ない

表 1 は、Yayla and Hu(2011)に基づいて著者が作成した。

表 2 情報セキュリティ事故

情報セキュリティ事故	説明
情報漏えい	組織内部の機密情報が外部に漏れてしまうこと。
不正アクセス	攻撃者がアクセス権限のない情報に不正にアクセスすること。
ウイルス感染	自分自身の複写、又は自分自身を変更した複写を他のプログラムに組み込むことによって繁殖し、感染したプログラムを起動すると実行されるプログラムがコンピュータシステムに入り込むこと。
DoS（攻撃）	攻撃者が目標のWebサイトに対して、膨大な数の要求パケットを送りつけることによりWebサーバを過負荷状態にして、Webサイトの本来のサービスを提供できないようにすること。
Webサイト改ざん	攻撃者が目標のWebサイトに対して、Webサイトの情報、たとえば記載内容やロゴなどを不適切な内容に書き換えたり、一部または全部のファイルを削除したり、Webサイトを停止させたりすること。

2.2 仮説 1

ある企業の株価のネガティブな反応の予測は、その企業の評価に対する効率的市場仮説 (Efficient Market Hypothesis . 以下, EMH) がベースに議論されている (Fama, 1970). EMH によれば、投資家は入手できるすべての情報を考慮して、企業価値を V_t と評価する。ここで V_t はある時点 t の将来のキャッシュフローの割引価値である。市場に新しい情報が公表された時、投資家は自らの評価を変更する。例えば、時点 $(t+1)$ の企業の価値は V_{t+1} となる。ここで V_t と V_{t+1} の差分 ΔV は新しい情報による企業価値の変化を表している。もしこの情報がポジティブだと考えられた場合には、 ΔV は正の値となる。情報セキュリティ事故の公表に対する株式市場の反応は、将来の企業の継続性と成長に関して投資家の見識が反映される。投資家は情報セキュリティ事故を当該企業の将来のキャッシュフローに対する潜在的な脅威と考えるので、 ΔV は負の値となる。企業固有の情報セキュリティ事故は明白なコストおよび実体のないコストの両方の原因となるので、投資家はそのようなコストを短期的には企業の業績に逆効果になると見なす。また現在のデジタル社会において企業にとって極めて重要な機密性の高い顧客情報や企業情報、情報資産などを守ることに企業が無力であると判明すれば、その企業の情報セキュリティ事故は長期的に、企業の株価に負の影響を与えると考えることができる。以上の議論から本研究では、まず「日本における情報セキュリティ事故の公表は、企業の株価に負の影響を与える」という仮説に焦点をあてた検証を行う。この仮説を以下では仮説 1 とする。

2.3 仮説 2

情報セキュリティ事故によって被害を受けた企業のソフトウェア製品、ハードウェア製品、たとえばオペレーティングシステム、ウイルス検出ソフトウェア、侵入検出ソフトウェア、ファイアウォールなどの有効性や信頼性について、顧客、ユーザ、投資家は疑問をもつと考えられる。しかしそのような製品の欠陥に加えて、情報セキュリティ事故は貧弱なセキュリティ管理が原因とも考えられる。適当なセキュリティポリシーやソフトウェアのパッチ管理を実装することに怠ったり、不適切な古い技術を使っているような企業では、情報セキュリティ事故を起こす可能性が高い。顧客や投資家はコンピュータやネットワーク、ソフトウェアを開発設計する IT 企業はセキュリティ管理が着実に実施されており、

非IT企業よりも情報資産を守っていると考えられる。したがってIT企業が自らのシステムやデータを守ることに失敗した時、投資家は情報セキュリティ事故に対して、非IT企業の場合よりもより強いネガティブな反応をすると考えた。EMHによれば、投資家は合理的な期待により、新しい情報によって自らの期待値を改める。したがってIT企業が情報セキュリティ事故を起こした場合には投資家の信用や信頼をより失う。そこで「情報セキュリティ事故の公表は、IT企業の事故の方がその他の業種タイプの企業の事故より、企業の株価により大きな負の影響を与える」という仮説を仮説2とする。

2.4 仮説3

最後に情報セキュリティ対策を着実に実施している企業に着目する。ISMS (Information Security Management System) 適合性評価制度は情報資産を様々な脅威から守り、リスクを軽減させるための総合的な情報セキュリティマネジメントシステムの運用を評価するものである。そして企業が積極的に情報セキュリティマネジメントシステム (PDCA サイクル) を回し、運用しているかが監査される。ISMSの構築と認証については日本工業規格の JIS Q 27001(ISO/IEC27001)という規格に準拠している。組織によって、その組織が所有する情報資産に対するリスク (情報漏えい, 紛失, 改ざんなど) は様々であり, 対応も多様である。ISMSでは各組織が各組織自体によるリスク評価に基づいて, 必要なセキュリティレベルを定め, 計画的に資源を配分して, 情報セキュリティマネジメントシステムを運用することを要求している。情報セキュリティ事故を予防するための処置を予防処置といい, これまでに実施していなかった新たな管理策を実施する。これは組織の戦略の変更や, 組織を取り巻く環境の変化に伴って新たな脅威やぜい弱性が対象となるためである。ISMS認証取得企業または組織が積極的に情報セキュリティ運用に取り組んでいる第1の理由は情報セキュリティ事故の予防である。これらの取得組織では情報セキュリティ事故発生による自社への影響度を十分に認識している。よって取得企業は情報セキュリティ事故を起こす確率も低いのではないかと考えられ, 投資家からすれば, この点においては信用・信頼を得ると考えられる。しかしこの信頼が裏切られた場合の失望感は未取得企業よりも大きく, 株価の大幅な下落に導くものと考えた。したがって「情報セキュリティ事故の公表は, ISMS認証取得企業の事故の方が未取得の企業の事故より, 企業の株価により大きな負の影響を与える」という仮説を仮説3とする。

次章で以上の3つの仮説について実証分析する。

3 実証分析

3.1 分析手法

3.1.1 イベントスタディ手法

本研究で使ったイベントスタディ手法について述べる。

企業*i*の情報セキュリティ事故 (イベント) の新聞発表日を $t = 0$ として, 企業*i*の株価収益率をマーケット・インデックスの収益率を用いて次の(1)式のようにモデル化する。

$$R_{it} = \alpha_i + \beta_i R_{mt} + \varepsilon_{it} \quad (1)$$

ここで、

R_{it} : t 日における企業 i の日次収益率

R_{mt} : t 日における市場(TOPIX)の日次収益率

ε_{it} : t 日における企業 i の誤差項

である。ただし、 t 日は企業 i のイベントの新聞発表日 ($t = 0$) からの相対である。たとえば $t = 10$ はイベントの新聞発表日から 10 日後を表す。

ここで $\hat{\alpha}_i$ と $\hat{\beta}_i$ を(1)式の最小自乗法を使って新聞発表日前のある期間で推定した値とすると、企業 i の t 日における収益率の理論値と実際の収益率との差、すなわち超過収益率 AR_{it} (Abnormal Return) は、

$$AR_{it} = R_{it} - (\hat{\alpha}_i + \hat{\beta}_i R_{mt}) \quad (2)$$

となる。なお今回の実証では、推定期間を $t = -220$ から $t = -20$ の 200 日間とした。

また超過収益率 AR_{it} を情報セキュリティ事故の新聞発表日 ($t = 0$) を含む期間 $[t_1, t_2]$ (イベントウインド) で集積した累積超過収益率 CAR_i は、

$$CAR_i = \sum_{t=t_1}^{t_2} AR_{it} \quad (3)$$

となる。さらにイベントウインド $[t_1, t_2]$ の全企業の累積超過収益率の平均値 $\overline{CAR}$ は、

$$\overline{CAR} = \frac{1}{N} \sum_{i=1}^N CAR_i \quad (4)$$

となる。同一企業で情報セキュリティ事故が複数回、発生する場合がある。その場合はそれぞれの事故に対して、各推定期間で、 $\hat{\alpha}_i$ と $\hat{\beta}_i$ を(1)式の最小自乗法で推測する。ただしイベントウインドと推定期間は重ならないとする。

3.1.2 イベントの抽出方法と結果

イベントの抽出は日経テレコン 2 1 を使用して行った。検出の期間は 1996 年 1 月 1 日から 2011 年 6 月 19 日である。検索キーワードは、

(個人情報 OR 顧客情報 OR 企業情報 OR 従業員情報) AND (流出 OR 漏えい)
および

不正アクセス OR ウイルス感染 OR Dos OR ((Web OR サイト) AND 改ざん)
である。本研究で扱った情報セキュリティ事故について表 2 にまとめた。

抽出の結果、4877 件の新聞記事を抽出した。抽出したイベントから推定ウインド及びイベントウインドの期間において株価が存在する日本の上場企業を抽出した。さらに、新聞記事の内容が重複するもの、推定ウインドがイベントウインドと重なるもの、イベントウインド期間内に、たとえば業績発表などの株価に影響を与えるような発表があったイベントを削除した。その結果、最終的にはイベント数 163 件、企業数 109 件、うち IT 企業 29 件、非 IT 企業 134 件、ISMS 取得企業 32 件、ISMS 未取得企業 131 件となった。なお IT

企業、非 IT 企業の分類は企業の東証の「業種分類」において“電気機器”及び“情報・通信業”である企業を IT 企業、それ以外を非 IT 企業とした。

3.1.3 平均の差の検定

仮説 2 と仮説 3 では、それぞれ 2 つのグループに分けてイベントスタディを行った。仮説 2 では IT 企業と非 IT 企業、仮説 3 では ISMS 認証取得企業と ISMS 認証未取得企業である。2 つのグループの $\overline{CAR}$ はイベントスタディ手法で算出できるが、この 2 つのグループの $\overline{CAR}$ に差があるのか、すなわち 2 つのグループで情報セキュリティ事故の公表が株価に与える影響に違いがあるのかを判断するには「平均の差の検定」を行う必要がある。そこで帰無仮説 (H_0 : 2 つのグループの $\overline{CAR}$ の差は 0 である) を立てて、分散が等しくないと仮定した 2 標本による t 検定を行った。

3.2 分析結果

3.2.1 仮説 1

抽出した全イベント 163 件の新聞発表に対する株価の反応を図 3 に示す。図 3 の横軸は新聞発表日の一日前（営業日）を t_1 とした場合 ($t_1 = -1$) の t_2 の値であり、縦軸はウィンド $[t_1, t_2]$ の $\overline{CAR}$ を示している。発表日翌日で -0.852%，5 日後では -1.106%，10 日後では -1.199% の下落となっており、それぞれ 1% 水準で有意であった。情報セキュリティ事故の発表後に株価が下落した結果は、仮説 1 の「日本における情報セキュリティ事故の公表は、企業の株価に負の影響を与える」を支持するものである。2004 年から 2008 年を期間として、主に情報関連産業を対象に検証した(高藪 et al., 2010)の報告と同様の結果となった。また Yayla and Hu(2011)が行った米国企業を対象にした 123 件の情報セキュリティ事故の分析と同様の結果が得られた。

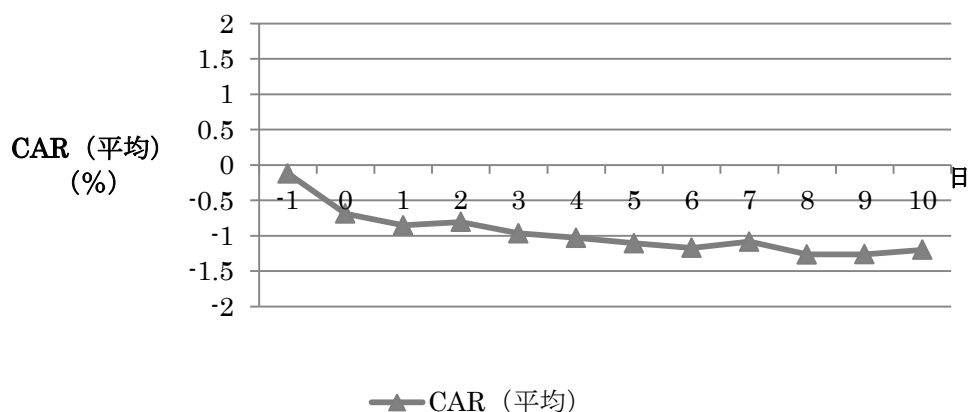


図 3 全情報セキュリティイベントの CAR (平均)

表 3 仮説 1・全情報セキュリティイベント

イベントウィンド	CAR(平均)	t値	p値
[-1,1]	-0.852	-4.729	0.0000 ***
[-1,5]	-1.106	-3.428	0.0004 ***
[-1,10]	-1.199	-2.909	0.0021 ***

***は 1%水準で有意であることを示している。

3.2.2 仮説 2

IT 企業が情報セキュリティ事故を発表した場合と非 IT 企業が情報セキュリティ事故を発表した場合に対する株価の反応を図 4 に示す。IT 企業の場合、 $\overline{CAR}$ の下落は翌日で-1.192%、5 日後で-2.352%、10 日後で-2.643%となり、非 IT 企業の場合は、翌日で-0.808%、5 日後で-0.887%、10 日後で-0.890%となった。いずれの下落も有意となっている。非 IT 企業では 3 日後で-0.878%の下落で、その後横ばい状態となっているが、IT 企業では 5 日後よりさらに 10 日後では下落の傾向があり、情報セキュリティ事故の公表に対する株価への負の影響が長期間にわたって継続していることがわかる。また IT 企業の場合と非 IT 企業の場合の平均の差の検定では、翌日では有意ではなかったが、5 日後、10 日後ではいずれも有意な結果となった。よって仮説 2 の「情報セキュリティ事故の公表は、IT 企業の事故の方がその他の業種タイプの企業の事故より、企業の株価により大きな負の影響を与える」を支持する結果となった。Yayla and Hu(2011)の分析では非 IT 企業は 5 日後、10 日後では $\overline{CAR}$ の下落は有意ではなく、結果が異なっている。

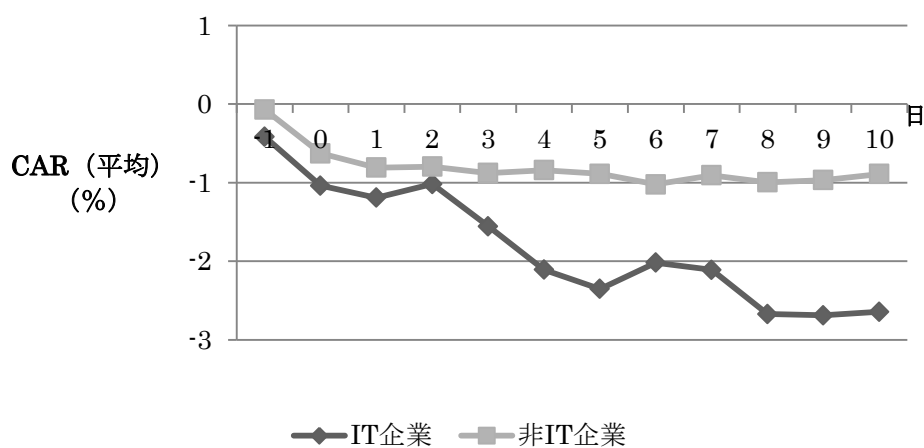


図 4 IT 企業と非 IT 企業の CAR (平均)

表 4 仮説2・業種タイプ別

イベント	イベント数	ウインドウ	CAR(平均)	t値	p値
IT企業	29	[-1,1]	-1.192	-2.305	0.0144 **
		[-1,5]	-2.352	-3.924	0.0003 ***
		[-1,10]	-2.643	-3.049	0.0025 ***
非IT企業	134	[-1,1]	-0.808	-4.298	0.0000 ***
		[-1,5]	-0.887	-2.419	0.0085 **
		[-1,10]	-0.890	-1.912	0.0290 **

***, **はそれぞれ 1%, 5%水準で有意であることを示している。

表 5 仮説2・平均の差の検定

ウインド		IT企業	非IT企業
[-1,1]	平均	-1.192	-0.808
	p値	0.490	
[-1,5]	平均	-2.352	-0.887
	p値	0.042	**
[-1,10]	平均	-2.643	-0.890
	p値	0.081	*

**, *はそれぞれ 5%, 10%水準で有意であることを示している。

3.2.3 仮説3

ISMS 認証を取得している企業が情報セキュリティ事故を発表した場合と ISMS 認証を取得していない企業が情報セキュリティ事故を発表した場合に対する株価の反応を図 5 に示す。ISMS 取得企業の場合、 $\overline{CAR}$ の下落は翌日で-1.191%, 5 日後で-2.272%, 10 日後で-2.899%であった。また ISMS 未取得企業の場合は翌日で-0.792%, 5 日後で-0.849%, 10 日後で-0.742%であった。いずれの下落も有意となっている。図 7 から ISMS 未取得企業の場合は、短期的な下落に止まり、翌日の-0.792%の下落後、ほぼ横ばいになっている。一方、ISMS 取得企業は 5 日後より 10 日後ではさらに下落しており、長期の間、情報セキュリティ事故の公表が影響していると考えられる。また ISMS 取得企業の場合と ISMS 未取得企業の場合の平均の差の検定では、翌日は有意ではなかったが、5 日後と 10 日後はいずれも有意な結果となった。よって仮説3の「情報セキュリティ事故の公表は、ISMS 認証取得企業の事故の方が未取得の企業の事故より、企業の株価により大きな負の影響を与える」を支持する結果となった。

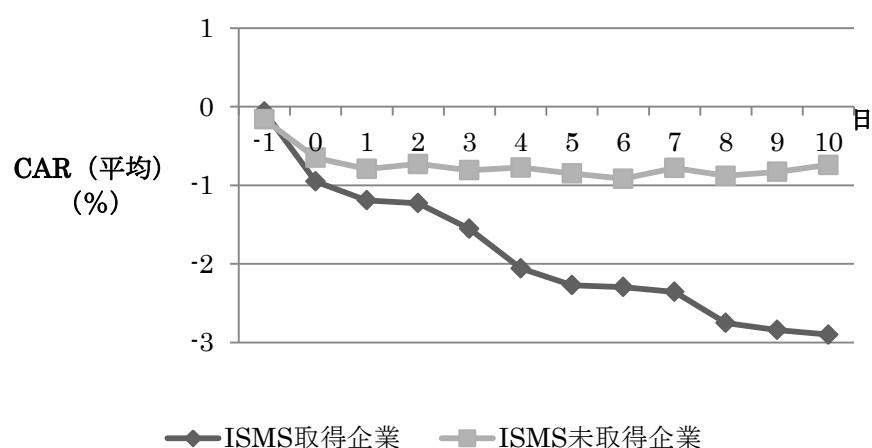


図 5 ISMS 認証取得企業と未取得企業の CAR (平均)

表 6 仮説 3・ISMS 認証取得の有無

イベント	イベント数	ウインドウ	CAR(平均)	t値	p値
ISMS取得企業	32	[-1,1]	-1.191	-2.516	0.0086 ***
		[-1,5]	-2.272	-3.900	0.0002 ***
		[-1,10]	-2.899	-2.606	0.0070 ***
ISMS未取得企業	131	[-1,1]	-0.792	-4.120	0.0000 ***
		[-1,5]	-0.849	-2.273	0.0123 **
		[-1,10]	-0.742	-1.696	0.0462 **

***, **はそれぞれ 1%, 5%水準で有意であることを示している。

表 7 仮説 3・平均の差の検定

ウインド		ISMS取得企業	ISMS未取得企業
[-1,1]	平均	-1.191	-0.792
	p値	0.439	
[-1,5]	平均	-2.272	-0.849
	p値	0.044	**
[-1,10]	平均	-2.899	-0.742
	p値	0.078	*

**, *はそれぞれ 5%, 10%水準で有意であることを示している。

4 おわりに

本研究では既存のイベントスタディ手法を使って、「日本における情報セキュリティ事故の公表は、企業の株価に負の影響を与える」という仮説を立てて検証した。その結果、情報セキュリティ事故を公表した企業の株価は、その直後に有意に下落していた。このことは、日本企業が情報セキュリティ事故を起こした場合、企業価値にネガティブに影響を与え得ると言える。また「情報セキュリティ事故の公表は、IT企業の事故の方がその他の業種タイプの企業の事故より、企業の株価により大きな負の影響を与える」という仮説を立てて検証した。その結果、IT企業、非IT企業ともに事故の公表直後に有意に下落していた。

しかも IT 企業と非 IT 企業の差の検定の結果、有意に差があり、IT 企業の方が非 IT 企業よりも有意に株価に与える影響が大きいことが明らかになった。情報セキュリティ事故は、たとえばオペレーティングシステム、ウイルス検出ソフトウェア、ファイアウォールなどの IT 製品と密接に関係している。IT 企業が自らの社内 IT システムに精通していることは当然であると考えられるので、企業が構築した社内 IT システムの有効性に顧客、ユーザ、投資家が疑問をもち、信用や信頼の失墜は非 IT 企業以上に大きいと考える。さらに「情報セキュリティ事故の公表は、ISMS 認証取得企業の事故の方が未取得の企業の事故より、企業の株価により大きな負の影響を与える」という仮説を立てて検証した。ISMS 認証取得企業は未取得企業よりも情報セキュリティに対する取り組みが投資家から信用・信頼を得ていると考えられるので、事故を起こした時の反動が未取得企業よりも大きいと考える。

本研究では2つのグループ間での平均の差の検定を行い、どちらのグループがより影響が大きいかを分析した。先行研究では差の検定を実施している例はなく、この点において本研究は新規性があるものとする。

本研究の課題は、情報セキュリティ事故の種別には焦点を当てていないことである。事故によっては企業価値に与える影響が違わないかという点、たとえば情報漏えい事故の場合とそれ以外の事故の場合の影響度に違いについてさらに詳細に検証していく必要がある。情報漏えい事故の影響が大きい仮定した場合、漏えいした情報の種別によっても株価の反応は違ふとさらに仮説を立てることができる。たとえば情報漏えい事故の場合、クレジットカード番号や銀行口座番号などの人の財産に脅威を与える種類の情報の漏えいは、その他の個人情報、たとえば氏名、生年月日、住所、電話番号、メールアドレスなどの情報漏えいよりも影響が大きいといった仮説を、イベントスタディ手法を使って検証できる。また仮説3で ISMS 認証取得企業の方が未取得企業よりも情報セキュリティ事故を公表した場合、株価への負の影響が大きいことが判明した。この結果を考慮すると株価の維持という観点からすると ISMS 認証を取得しない方が得策であると言える。そこで ISMS 認証取得企業は情報セキュリティ事故を発生させる可能性が低いことが言えれば、ISMS 認証の取得の意義を主張できると考える。よって今後、ISMS 認証の取得の有無と情報セキュリティ事故の発生の可能性について検証を進める必要がある。

著者は経済産業省が実施した平成21年度情報処理実態調査の個票データを統計的に分析して、組織的対策への情報セキュリティ投資がセキュリティ事故の防止に効果的であることを明らかにした。そして本研究では情報セキュリティ事故の公表が企業価値に負の影響を与えることを明らかにした。すなわち適切な情報セキュリティへの投資が事故を防止し、その結果、企業価値を維持する要因の一つになることを、実際のデータを用いて統計的に示すことができた。以上の成果が、企業が情報セキュリティへの投資や事故予防の活動に積極的に取り組むことへの動機付けになれば本研究は意義のあるものだと考える。

(参考文献)

- Benbunan-Fich, R. and Fich, E. M. (2004). Effects of Web Traffic Announcements on Firm Value. *International Journal of Electronic Commerce*, 8, 161-181.
- Campbell, K., Gordon, L. A., Loeb, M. P. and Zhou, L. (2003). The Economic Cost of Publicly Announced Information Security Breaches: Empirical evidence from the stock market. *Journal of Computer Security*, 11, 431-448.
- Cavusoglu, H., Mishra, B. and Raghunathan, S. (2004). The Effect of Internet Security Breach Announcements on Market Value: Capital market reactions for breached firms and internet security developers. *International Journal of Electronic Commerce*, 9, 70-104.
- Dehning, B., Richardson, V. J. and Zmud, R. W. (2003). The Value Relevance of Announcements of Transformational Information Technology Investments. *Mis Quarterly*, 637-656.
- Dutta, A. and Mccrohan, K. (2002). Management's Role in Information Security in a Cyber Economy. *California Management Review*, 45, 67-87.
- Ernst & Young (2003). *Global Information Security Survey 2003*, London, UK, Ernst & Young LLP.
- Ernst & Young (2008). *Global Information Security Survey 2008*, London, UK, Ernst & Young LLP.
- Ettredge, M. L. and Richardson, V. J. (2003). Information Transfer among Internet Firms: The case of hacker attacks. *Journal of Information Systems*, 17, 71-82.
- Fama, E. F. (1970). Efficient Capital Markets: A review of theory and empirical work. *The journal of Finance*, 25, 383-417.
- Garg, A., Curtis, J. and Halper, H. (2003). Quantifying the Financial Impact of IT Security Breaches. *Information Management & Computer Security*, 11, 74-83.
- Gordon, L. A., Loeb, M. P. and Sohail, T. (2010). Market Value of Voluntary Disclosures Concerning Information Security. *Mis Quarterly*, 34, 567-594.
- Hovav, A. and D'arcy, J. (2003). The Impact of Denial of Service Attack Announcements on the Market Value of Firms. *Risk Management and Insurance Review*, 6, 97-121.
- Hovav, A. and D Arcy, J. (2004). The Impact of Virus Attack Announcements on the Market Value of Firms. *Information Security Journal: A Global Perspective*, 13, 32-40.
- Khansa, L. and Liginlal, D. (2009). Quantifying the Benefits of Investing in Information Security. *Communications of the ACM*, 52, 113-117.
- McWilliams, A. and Siegel, D. (1997). Event Studies in Management Research: Theoretical and empirical issues. *The Academy of Management Journal*, 40, 626-657.
- Mercuri, R. T. (2003). Analyzing Security Costs. *Communications of the ACM*, 46, 15-18.

- Nash, S. K. 2008. The Global State of Information Security. *CIO Magazine*.
- Ohlson, J. A. (2001). Earnings, Book Values, and Dividends in Equity Valuation: An Empirical Perspective. *Contemporary Accounting Research*, 18, 107-120.
- Subramani, M. and Walden, E. (2001). The Impact of E-commerce Announcements on the Market Value of Firms. *Information Systems Research*, 12, 135-154.
- Yayla, A. A. and Hu, Q. (2011). The Impact of Information Security Events on the Stock Value of Firms: The effect of contingency factors. *Journal of Information Technology*, 26, 60-77.
- 高籾, 学., 澤谷, 拓. and 村田, 晴. (2010). 情報セキュリティ投資の企業価値に与える影響ーイベントスタディによるー. *証券経済学会年報*, 158-164.
- 独立行政法人情報処理推進機構 (IPA) (2010). *情報セキュリティ白書 2010*.

-
- i 「2010 年国内情報セキュリティ市場 企業ユーザ動向調査：セキュリティ投資の動向」(IDC Japan)
- ii 「企業の情報セキュリティ投資によるセキュリティ効果の実証研究」(青山学院大学 2010 年度国際マネジメント研究科研究奨励賞応募論文)
- iii NPO 日本ネットワークセキュリティ協会による想定損害賠償額算定の方法
- (1) 事前調査
報道されたセキュリティ事故を調査・集計する。同時に過去のプライバシー権侵害や名誉毀損の判例を調査する。ここでは「宇治市住民基本台帳データ大量漏えい事件控訴審判決 大阪高等裁判所 平成 13 年 (ネ) 第 1165 号 損害賠償請求控訴事件」を参考にした。
 - (2) 分析
集計した事故の被害者数, 漏えい情報種別, 漏えい原因, 漏えい経路などを分析する。
 - (3) 算出式作成
算出式の入力項目を決定し, 算定式を策定する。入力項目は, 漏えい情報の価値, 漏えい組織の社会的責任度, 事後対応評価とした。また, 弁護士などの専門家の意見も取り入れた。
 - (4) 検証
策定した算定式の信憑性をはかるため, 先の宇治市の事例に当てはめ, 算定式で得られた結果と実際の判決による損害賠償額と比較した。Yahho!BB, 及び TBC の判決との比較も行った。その結果, 同程度の数値が得られた。
なお算定結果は, あくまでも「もし被害者全員が賠償請求したら」という“仮定”に基づくものであり, 実際に各事故においてその金額が支払われたものではない。
- iv 「情報セキュリティ事故に関する調査報告書」(2002～2010 年度) (NPO 日本ネットワークセキュリティ協会) に基づいて, 筆者作成。
- v 「一人当たりの平均想定損害賠償額」は, 事故毎の「一人当たりの想定損害賠償額」の平均金額である。よって全事故の「一人当たりの想定損害賠償額」を合計し, 「事故総件数」で除算して, 「一人当たりの平均想定損害賠償額」を算出している。「想定損害賠償額の合計」を「漏えい人数の合計」で除算した値ではない。
- vi 「情報セキュリティ事故に関する調査報告書」(2002～2010 年度) (NPO 日本ネットワークセキュリティ協会) に基づいて, 筆者作成。