◇ KDDI総研R&A　　2006年11月第2号

情報セキュリティ投資に対する企業の意志決定

記事のポイント

サマリー

情報セキュリティ障害は、長年築きあげてきた「信頼」が一瞬にして瓦解してしまうほど企業にとって大きな影響力を持つ。それゆえ、情報セキュリティ対策が経営上の問題として重要視されている。特に、「情報」を直接扱う企業においては、細心の注意を払ってセキュリティ対策が講じられている。しかしながら、どの程度対策にお金をかけるべきか、ということに対する明確な判断基準が確立されていないため、情報セキュリティに対するリスクを認識しながらも、適切な情報セキュリティ投資がなされていないケースも多いのではないだろうか。

本稿では、情報セキュリティ投資が、一過性の費用というよりは、むしろ「投資」としての性質が強く、適切な情報セキュリティ投資が企業価値を高めること、また、情報セキュリティ対策の組み合わせによってもその効果が異なることを、先行研究のサーベイを中心にレポートする。これらを通じて企業における適切な情報セキュリティ投資の意志決定の一助となれば幸いである。

キーワード　情報セキュリティ投資　情報セキュリティ障害　企業価値　意志決定

地　域　米国　日本

執筆者　KDDI総研　第2市場分析室　藤原　正弘（fujiwara@kddi.com）

はじめに

情報セキュリティに対する適切な投資額は、その企業の置かれた情報セキュリティリスクの状況、施されるセキュリティ対策の効果、その企業が守るべき企業価値などによって決定されるだろう。しかしながら、そうした指標は、少なくとも現時点では、簡単には得られない。だからといって、全く手掛かりがないわけではない。情報セキュリティ投資の研究分野はまだ歴史が浅いが、情報セキュリティ投資の意志決定に役立てられる判断材料を提供し始めている。

本稿では、適切な投資の判断材料として、いくつかの研究論文を紹介するが、第1章では、米国における情報セキュリティ障害がもたらした企業価値の損失を推計した論文を紹介し、企業の「信用」や「信頼」が、財務諸表には計上されないものの、少なからぬ資産規模を有することを示す。つづく第2章では、講じる対策の組み合わ

せによって効果が異なることを実証した論文を紹介し、投資額のみならず、情報セキュリティ対策の種類についても重要な経営上の意思決定であることを示す。最後の第3章では、企業価値と資本ストックについて説明し、情報セキュリティ投資が保険のような受動的な意味を超えて、情報セキュリティを確保すること自体が、企業価値を高める積極的な投資の側面を持つことを明らかにする。

1　情報セキュリティ障害によって失われる企業価値

2000年2月に、米国の代表的なインターネット企業であるAmazon、eBay、yahoo!などが、いわゆるDos攻撃☞（用語）を受けたことが大きな話題となり、これを契機に情報セキュリティ投資に対する認識が高まった。

Cavusoglu他[2004]の論文では、1996年から2001年の間に発生した情報セキュリティ障害によって、どれだけの損失が発生したかを推計している☞（脚注１）。それによると、障害が発生した事実が公表されてから2日の間に平均2.1%の株価の下落を観測している。この下落率は、1件の障害が、平均16.5億ドル（1ドル＝115円換算で、約1,798億円）の時価総額の損失に相当する。☞（脚注２）

情報セキュリティ障害によって企業価値が損なわれるメカニズムは、短期的なインパクトと、長期的なインパクトの、2つに分けて考えることができる。短期的なイ

📖
☞（用語）　Dos攻撃
あるサイトに対して集中的にアクセスを仕掛けることで一般利用者がほとんど利用できなくさせること。Denial Of Service attacksの略。

☞（脚注１）
この論文では、情報セキュリティ障害の特定は３つのニュースソース（Lexis/Nexas,CNET,ZDNET）における障害報道に基づいている。”attack” ”breach” “break-in” “hacker” “Internet” “security”といった情報セキュリティ障害に関わるキーワードが含まれる記事を抽出した結果、1996年から2001年の6年間に2,563件見つけている。これらから重複や単なるハード障害などを除外し、さらに、株価へのインパクトを推計することから政府機関やNPOなどを除外して、最終的には66件の情報セキュリティ障害を特定している。
66件の内訳は、サービス停止を狙った情報セキュリティ攻撃が34件、その他が32件となっている。発生年次別にみると、1999年までは年数件だが、2000年は21件、2001年は26件と急激に増加している。

☞（脚注２）
2002年2月のDos攻撃による、yahoo!、eBay、Buy.comの株価の下落率はそれぞれ15%、24%、44%にもなった。（Atomic Tangerine[2000],"NPV: Information Security”）
”CSI-FBI Computer Crime and Security Survey 2006”には企業アンケートによる損失額が報告されている。それによると、616の企業からの回答のうち、74%の企業は何らかの金銭的損失を被ったが、推定額を回答したのは51%の企業（313社）だけである。推定できた損失額の総額は$52,494,290（約60億円：¥115/$換算以下同じ）、 1社当たり平均$167,713（1,929万円）となっている。障害1件あたりの損失額の平均は、不正アクセスが$85,621（985万円）、ウィルス被害が$69,125（795万円）、ノートパソコンなどモバイル機器の盗難が$30,057（346万円）、DOS攻撃が$20,872（240万円）となっている。

ンパクトとは、サービス停止による売上減や復旧作業に要した費用、お客様からの問い合わせ対応の費用など、いずれも金額として算出可能なものである。これに対して、長期的なインパクトは、将来の利益を減少させるような要因である。たとえば、これを契機に他社に移ったお客様からあげられるはずであった収益、失ってしまったお客様やパートナー企業の信頼などである。

また、Cavusoglu他[2004]の分析からは次のような傾向が見られることもわかっている。

- 情報セキュリティ障害による損失額は、一般企業よりもインターネット企業のほうが高額になる。
- 損失額は年々高額になる。
- 大企業よりも中小企業において損害の影響が大きい。☞（脚注１）
- 損失額の情報セキュリティ障害の種類による違いは明らかでない。☞（脚注２）

こうした企業価値の減少要因を市場が評価した結果が、上記の時価総額における損失となって現れるのである。これらの推計値から、「信用」や「信頼」の喪失が大きな企業価値の減少をもたらすものであることがよくわかり、ここに情報セキュリティ投資に対する経済合理性の観点での根拠がある☞（脚注３）。これらの金額は、情報セキュリティ投資の意志決定に際し、ひとつの判断材料となるものであろう。

2　情報セキュリティ投資の効果的な組み合わせ

情報セキュリティ対策としては、ファイアウォールに代表されるハードウェア装置や、ウィルス対策のソフトウェアなど、セキュリティ対策開発企業の製品を購入する方法が想起されやすいが、企業内のセキュリティポリシーの構築や、社員への情報セキュリティ教育などの施策についても重要な鍵を握っていることがわかって

☞（脚注１）

中小企業は大企業に比べると相対的に経営基盤が弱いため、情報セキュリティ障害の種類に関わらず、影響の度合いが大きいことが考えられる。

☞（脚注２）

現実にはセキュリティ障害の内容によって損失額が大きく異なることが想定されるが、セキュリティ障害の詳細と具体的な損失額が得られないので、詳細な分析はなされていない。

☞（脚注３）

情報セキュリティの問題では、コンピュータウィルスのように他者に対する迷惑を発生させるケースもあり、自社の経済合理性だけで投資の正当性を論ずることは不十分だと考えるが、仮に他者を顧みない独善的な企業であっても、市場評価という限られた観点から考えても投資の根拠があるということである。

きている。

田中[2005]では、経済産業省の「情報処理実態調査」のデータを用いて、コンピュータウィルスによる被害を対象に、情報セキュリティ対策の組み合わせによって効果に違いがあるかどうかを検証している。田中[2005]によると、情報セキュリティポリシーの構築・維持や情報セキュリティ教育なども同時に行うことは、ウィルス被害に対する効果を上昇させるが、ファイアウォール(FW)を導入するだけでは、むしろ効果が小さくなることが報告されている(図表1の⑧項)。さらに、Liu他[2006]は単年度だけ対策を講じた場合と、2年続けて対策を講じた場合を比較し、単年度の場合は明らかに効果が減ずることを確認している。

ここではウィルス被害だけを調査対象としているが、情報セキュリティに対する具体的な施策の面においても、設備による対応と人的対応の両方の側面で対策を講じることが高い効果を生むのである。

【図表1】 各対策が情報セキュリティ安全度指標に及ぼす効果

(αは「情報システム脆弱性指標」、βは「電子メールID数」、γは「対策の種類①~⑫」のそれぞれの係数推計値および有意度を表す)

対策の種類	導入率%	α	β	γ	調整済みR²
①セキュリティ・ポリシー策定	45.8	-0.129***	-0.824***	0.647	0.13
②セキュリティ・ポリシー定期的見直し	21.9	-0.129***	-0.828***	1.045***	0.13
③全社的なセキュリティ管理者配置	48.2	-0.127***	-0.822***	0.325	0.13
④部門毎セキュリティ管理者配置	28.7	-0.128***	-0.829***	0.740***	0.13
⑤従業員に対するセキュリティ教育	33.2	-0.127***	-0.828***	0.508**	0.13
⑥重要なコンピュータ室への入退出管理	49.6	-0.127***	-0.853***	0.521**	0.13
⑦重要なシステムへの内部アクセス管理	66.6	-0.126***	-0.810***	-0.085	0.13
⑧外部接続へのFWの設置	77.2	-0.124***	-0.809***	-0.809***	0.13
⑨セキュリティ監視ソフトの導入	52.7	-0.126***	-0.815***	0.122	0.13
⑩外部専門家による常時セキュリティ監視	14.0	-0.128***	-0.822***	0.620**	0.13
⑪外部専門家による定期的なシステム監査	18.1	-0.127***	-0.822***	0.375	0.13
⑫内部による定期的なシステム監査	21.5	-0.126***	-0.815***	0.071	0.13

(注) 導入率(%)=(当該対策を導入している企業数)/(全サンプル数:3,151社)×100
***:p値0.01未満、**:p値0.05未満、*:p値0.1未満

(図表の解説) 対策の種類①~⑫をひとつずつ回帰させた結果を表す。それぞれの対策が安全度指標にプラスに影響を与える場合、γの符号が正で"*"が付く。すなわち、②④⑤⑥⑩が統計的に効果のある対策と判断できる。一方、⑧は"*"が付いているが符号が負であるため安全度指標にマイナスの影響を与えると判断できる。
さらに、本表には掲載されてないが、①⑤⑧の組み合わせが有効であることが確認されている。

(出典) 田中[2005], 図表8

3　企業価値

第1章で取り上げた時価総額の損失に対する情報セキュリティ投資という観点は、保険の考え方に似ているが、本来的には、災害や事故に比べれば、情報セキュリティへの対策と効果は確実性が高いものと考えられる。すなわち、しっかり対策を講じておくことが、企業の安定性を高め、経営基盤を厚くする活動として認知されてもよいのではないだろうか。第3章では、情報セキュリティ投資が直接「企業価値」を高める「投資」としての役割を持つことを説明する。

企業価値の指標にはいろいろな尺度が考えられるが、ここでは株式市場における評価を考える。具体的には、時価総額（＝株価×発行株数）で示されると考える☞（脚注１）。簡便に書くと、投資理論では、

時価総額＝企業が得るであろう将来の利益の現在価値

としている。ただし、時価総額が大きいから企業価値が高いのではなく、企業価値が高いから時価総額が大きくなる。

一方、企業は利益を出すために、資本や労働といった生産要素を活用して財やサービスを生産する。これらの生産要素は、資本ストックが貸借対照表に計上されるように、有価証券報告書などで公開されている。投資家の立場で考えてみると、より少ない資本でより多くの利益をあげる企業に投資するのが合理的である。そこで、時価総額（資本家の投資額の総額）と資本ストックを比較して考えると、時価総額が資本ストックを下回る状況では、企業は事業を続けるよりも資本ストックを売却したほうが、利益がでることを意味している。一般的には、時価総額が資本ストックを上回っており、企業が資本ストックを使って財やサービスを生産することのほうが資本ストックを売却するより利益を生み出す、と投資家（市場）が評価していることを示している。☞（脚注２）

1990年代より情報技術が企業活動に浸透するに従って、時価総額と資本ストックの乖離が大きくなっていることを、Hall[2001]の研究は明らかにしている。Hall[2001]では、「財務諸表には現れない資本ストックの割合が高くなった」と市場が評価したため、と解釈している。財務諸表に現れない資本というのは、たとえば、従業員のスキル、企業の組織構造、生産プロセス、企業文化、企業の信用、広告宣伝といったものを指している。これらは、企業が何らかの費用を投じるものの、明確な形をもってその成果を表すことが困難であり、かつ、一過性の現象ではなく企業の中や

☞（脚注１）

市場が評価する企業価値といった場合には、債務についても考慮が必要だが、ここでは省略している。

☞（脚注２）

時価総額と資本ストック（資本の再取得価格）の比率は「トービンのｑ」として知られている。（J. Tobin[1969],"A General Equilibrium Approach to Monetary Theory", *Journal of Money, Credit and Banking*, vol.1, no.1, pp.15-29）

周辺に蓄積し、企業活動にプラスの貢献を及ぼす性質を持つものである。こういった資本を「インタンジブル・アセット（見えない資本)」と呼ぶ。☞（脚注１）

現実の市場においては、インタンジブル・アセットに投資する企業に高い評価が与えられることも多く、米国経済においては、人的資本ストックが物的資本ストックを上回っているという論文も発表されている。☞（脚注２）

本稿のテーマである情報セキュリティも、入退室管理システムやファイアウォールといった有形資産の部分もあるが、セキュリティポリシーの構築・維持や情報セキュリティ教育の充実などインタンジブルな部分も多くある。さらに、情報セキュリティへの投資額の大きさが単純にセキュリティの高さに通じるものでないだけに、市場にとっても有形資産のように評価することは困難であろう。

しかし、情報セキュリティへの投資は、企業にとって重要なインタンジブル・アセットである「信用」や「信頼」を維持するために必要不可欠な継続的企業活動のひとつであり、それにかかるコストはその場限りで消費されるものではなく、目に見えない形で業務プロセスや企業文化の中に蓄積していくものである。すなわち、情報セキュリティが維持されていること自体がインタンジブル・アセットであるということができる。高い情報セキュリティを維持することが、直接企業価値を高めるという積極的な役割も担っているのである。

これに関して、Tanaka and Ueno[2006]では、経済産業省が行っている「情報処理実態調査」のデータを用いて、情報投資に占める情報セキュリティ投資の割合が高いほど、市場で評価される企業価値が高くなることを実証的に示しており☞（脚注３）、情報セキュリティへ対策を講じることが「インタンジブル・アセット」として市場からプラスの評価を得ることが明らかになっている。

情報セキュリティ投資が企業活動に必要な投資であるのはよいとして、実際問題は、どのようなセキュリティ対策にどれくらい投資を行うことが、（少なくても経済的に）合理的であるのかということである。現時点では、情報セキュリティ投資の直接的な費用対効果の評価手法は確立されておらず、研究者や政策立案者の今後の研究が期待される。

☞（脚注１）

最近では、この「見えない資本」を見えるようにすることが企業の競争力を高めるという議論も行われている。「可視化」「ビジブル（visible)」「見える化」といったキーワードがよく使われる。

☞（脚注２）

Jorgenson, Dale W., and Barbara M. Fraumeni [1995], “Investment in Education and U.S. Economic Growth”, Productivity, Volume 1: Postwar U.S. Economic Growth, edited by D. W. Jorgenson, MIT Press.

☞（脚注３）

説明変数を「情報投資に占める情報セキュリティ投資の割合」、トービンのｑを被説明変数として回帰分析を行っている。

本稿では、研究論文を中心に情報セキュリティ対策の意志決定における判断材料を提示してきたが、あらためてまとめると、以下の３つに集約される。

① 企業にとって「信用」「信頼」に起因する損失額は極めて大きい。

② ハードやソフトの対策だけでなく、組織管理や人材育成における対策と組み合わせて継続的に実施することが高い効果を生む。

③ 情報セキュリティ対策は、それ自体、インタンジブル・アセットとして企業価値を高める（市場が評価する）。

出典・参考文献

Cavusoglu, Huseyin, M. Birendra and S. Raghunathan [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*, Fall 2004, vol. 9, No. 1, pp.69-104

CSI(Computer Security Institute), “CSI/FBI COMPUTER CRIME AND SECURITY SURVEY 2006”

Hall, Robert E.[2001], “The Stock Market and Capital Accumulation”, *American Economic Review* 91(5), pp.1185-1202

Liu, Wei, H. Tanaka and K. Matsuura [2006], “An Empirical Analysis of Security Investment in Countermeasures Based on an Enterprise Survey in Japan”, WEIS 2006, 26-28 June

Tanaka, Hideyuki, K. Matsuura and O. Sudoh [2005], “Vulnerability and information security investment: An empirical analysis of e-local government in Japan”, *Journal of Accounting and Public Policy*, 24(2005), pp.37-59

Tanaka, Hideyuki, K. Ueno [2006], “Information Security Investment and Firm Value as Measured by Tobin’s q”, 3rd Forum on Financial Systems and Cyber Security, May 24, 2006

エリック・ブリニョルフソン（CSK訳・編），『インタンジブル・アセット：「IT投資と生産性」相関の原理』，ダイヤモンド社，2004年

田中秀幸[2005]，「インタンジブル・アセットとしての情報セキュリティ　ー情報セキュリティ投資に関する企業レベルの実証分析ー　」，東京大学大学院情報学環紀要No.69，2005年3月

【著者紹介】
氏　　名：藤原　正弘（ふじわら　まさひろ）
所　　属：KDDI総研 第2市場分析室 研究主幹
専　　門：情報通信全般の社会・経済分析
調査報告書　「アジア諸国においてITが社会経済の成長に貢献した役割」調査報告書（2004年3月）（ICF：国際コミュニケーション基金）
「携帯電話サービスにおけるネットワーク外部性の推計」（2005年3月）（ICF）
「電気通信サービスの現状」調査報告書（2006年3月）（総務省）
調査レポート　「地球上にある、情報の「量」を推計する」KDDI総研R&A誌2004年3月号
「携帯電話におけるプラットフォーム戦略の分析」 R&A誌2005年5月号
「携帯電話の価格指数の分析」 R&A誌2005年10月号
「ヘドニック価格分析による携帯電話の機能評価」 R&A誌2005年11月号
「プラットフォームビジネスにおける企業連携」 R&A誌2006年3月号
所属学会　情報通信学会、日本社会情報学会（JASI）、社会経済システム学会
その他　KDDI広報誌「Time&Space」誌コラム連載
Email　：fujiwara@kddi.com
電話　：03-6716-1152