RCSSディスカッションペーパーシリーズ
第49号　2007年2月

ISSN 1347-636X

Discussion Paper Series
No.49 February, 2007

情報セキュリティ投資の経済分析

竹　村　敏　彦

RCSS

文部科学省私立大学学術フロンティア推進拠点
関西大学ソシオネットワーク戦略研究センター

Research Center of Socionetwork Strategies,
The Institute of Economic and Political Studies,
Kansai University
Suita, Osaka 564-8680 Japan
URL : http://www.rcss.kansai-u.ac.jp/
http://www.socionetwork.jp/
e-mail : rcss@jm.kansai-u.ac.jp
tel. 06-6368-1228
fax. 06-6330-3304

情報セキュリティ投資の経済分析

竹　村　敏　彦

RCSS

文部科学省私立大学学術フロンティア推進拠点
関西大学ソシオネットワーク戦略研究センター

Research Center of Socionetwork Strategies,
The Institute of Economic and Political Studies,
Kansai University
Suita, Osaka 564-8680 Japan
URL : http://www.rcss.kansai-u.ac.jp/
http://www.socionetwork.jp/
e-mail : rcss@jm.kansai-u.ac.jp
tel. 06-6368-1228
fax. 06-6330-3304

情報セキュリティ投資の経済分析*

竹村敏彦†

関西大学ソシオネットワーク戦略研究センター‡

E-mail: takemura@rcss.kansai-u.ac.jp

2007年2月

概 要

情報通信技術の進展は組織などの生産性や効率性を上昇され、社会はインターネットに強く依存する状態になっている。一方で、インターネットの脅威も拡大し、その問題は深刻化している。本稿では、情報通信技術がもたらす正の経済効果に注目するのではなく、負の経済効果に注目し、理論研究かつ実証研究に関するサーベイを与える。つまり、情報セキュリティ投資の経済分析の概論を与える。また、費用対効果の観点から軽視されがちにある情報セキュリティ投資を事業継続正の観点から考察をおこなっている。そして、情報セキュリティ対策の課題と今後の展望について議論をおこなっている。

KEYWORD: 情報セキュリティ, インターネット, 重要インフラ, 事業継続性, 企業価値

*本稿は、文部科学省の科学研究費補助金交付課題「情報インフラにおけるセキュリティ投資の経済分析」（課題番号18730202・若手研究 (B)・研究代表者 竹村敏彦）の研究成果である。なお、草稿において宗岡徹（関西大学・教授）、横見宗樹（大阪商業大学・専任講師）、江良亮（山形県立産業技術短期大学・専任講師）、坂本博史（財団法人国際通信経済研究所・上級研究員）、部奈和洋（大和住銀投信投資顧問会社）の諸氏から有益なコメントをいただいた。ここに記して深く感謝の意を表したい。

†関西大学ポスト・ドクトラル・フェロー

‡〒 564-8680 大阪府吹田市山手町 3-3-35 関西大学経済・政治研究所ソシオネットワーク戦略研究センター

Economic Analysis of Information Security Investment

TOSHIHIKO TAKEMURA
Postdoctral Fellow, Research Center of Socionetwork Strategies, Kansai University
E-mail: takemura@rcss.kansai-u.ac.jp

February, 2007

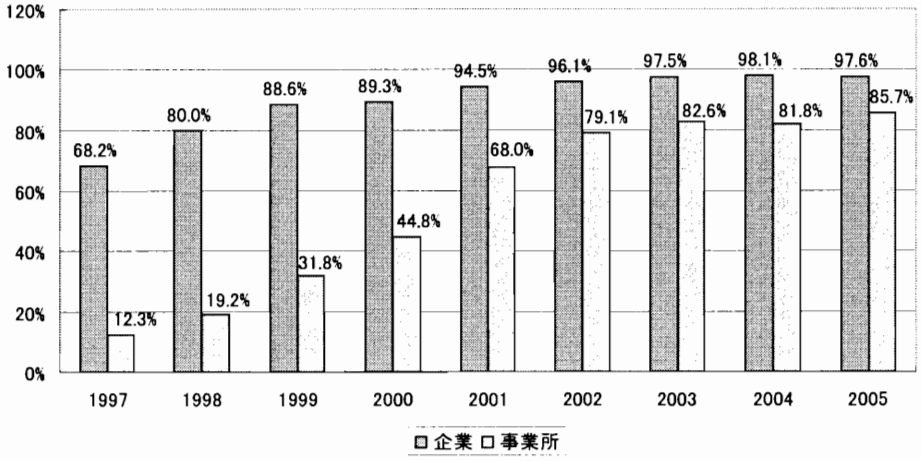
Abstract

The progress of the information and communications technology (ICT) rises productivity and the efficiency in the organizations, and the society and economy depends on the Internet strongly. On the other hand, the threats of the Internet expands and the problem has become aggravated. In this paper, we focus on negative economic effect, not positive economic effect on the ICT. We give survey on theoretical and emperical studies concerning with information security investment. In other words, we show the outline of economic analysis on information security investment. Moreover, we discuss information security investment from viewpoint of business continuity. Finally, we discuss the problem on the information security measures and the view in the future.

KEYWORD: Information Security, Internet, Critical infrastructure, Business Continuity, Market Value

1 はじめに

1980年代後半から議論され続けた情報通信技術（ICT; Information and Communication Technology）の生産性について多くの実証研究がおこなわれて、20世紀の終わりにその有効性が確認されるようになった[1]。これらの研究では、ICT投資をすることで企業や産業、経済全体の生産性や効率性を向上させることができると主張されている。そして、e-Japan計画やブロードバンドの普及とあいまって、ビジネス分野における企業情報システムの形態が大きく変化し、ICT投資が盛んにおこなわれるようになった[2]。特に、EDI（Electronic Data Interchange）などの企業間の連携に代表されるB2B（Business to Business）やオンラインショッピングなどのB2C（Business to Consumer）が活発化して、業種を問わず、インターネットを介して様々なビジネスが急成長を遂げてきた[3]。また、ここ数年の間に、社会はインターネットに強く依存していることが指摘されている[4]。図1からもその動向を捉えることができる。図1を見てわかるように、1997年において



総務省 (2002, 2005, 2006) より作成

図 1: 企業・事業所のインターネット導入率

68.2%であった企業のインターネット導入率は2005年には97.6%となり、ほぼ全ての企業において

[1] 日本のICT投資に関する先行研究については江良・竹村 (2005) や竹村 (2006a) などを参照されたい。

[2] 高度情報通信ネットワーク社会推進戦略本部（IT戦略本部）は、ICTの活用により世界的規模で生じている急激勝つ大幅な社会経済構造の変化に的確に対応することの緊要性に鑑み、高度情報通信ネットワーク社会の形成に冠する施策を迅速かつ重点的に推進するために設立された。IT戦略本部のホームページは、http://www.kantei.go.jp/jp/singi/it2/index.htmlである。

[3] これらの動向については、総務省 (2006) を参照されたい。

[4] 山口 (2007) などを参照されたい。

インターネットは利用されている状況にある。また、事業所のインターネット導入率は1997年の12.3%から8年間で85.7%にまで急激に増加している。主としてそのようとは、ASP（Application Service Provider）やiDC（internet Data Center）の利用、B2BやB2Cなどの新たなるビジネスモデルを視野に入れたものとなっている。

しかしながら、近年のインターネットやICTの利用に関する深刻な社会問題が浮上している。それらは情報セキュリティに関するものである。具体的には、CodeRed、Blaster、Nimdaなどに代表されるコンピュータウィルス、クラッキングや盗聴などの不正アクセス、DoS（Denial of Service）やIPスプーフィング（IP Spoofing）などの攻撃、WinnyやWinMXに代表されるP2P（Peer to Peer）の普及にともない拡大したボットネット（Botnet）、フィッシング（Phishing）、マルウェア（Malware）、スパムメール（Spam Mail）などの様々なインターネットの脅威である[5]。情報処理推進機構（IPA; Information-Technology Processing Associate）やJPCERT/CC（Japan Computer Emergency Response Team/Coordination Center）が公開しているコンピュータウィルスや不正アクセスなどの情報セキュリティインシデントに関する問い合わせ件数は年々増加傾向にある[6]。あくまでこれらの数値は問い合わせであり、氷山の一角でしかないと思われる。実際に、2000年以降、これらが原因で個人や企業をはじめとする組織の重要情報（機密情報）が漏洩したり、またシステムをダウンさせ、経済活動をできないようにするといった情報セキュリティ被害が国内外で相次いでおこっている[7]。さらに、昨今これらの脅威は高度化し、また相互に関連しシステマティックなものとなっており、インターネット利用者にとって更なる脅威となっている。このような環境において、企業はこれらの脅威から投資したICT試算や情報を防護しなければ、社会的信頼の失墜や膨大な（金銭的な）損失を被る危険性に直面することになる。それゆえに、企業は防護のために十分や情報セキュリティ投資を行う必要がある。しかしながら、実際、費用対効果の観点から、情報セキュリティ投資は他の投資に比べて重要視されているとはいいがたい[8]。ここで、情報セキュリティ投資とは「所有するサーバやコンピュータ、情報を様々な脅威から防護するための管理システムを導入したり、それらを運用管理また利用する教育をおこなうための投資」のことを意味する。なお、情報セキュリティおよび情報セキュリティ投資の定義は次節で与える。

この状況を踏まえて、本稿では情報セキュリティを経済学的にとらえた概論を与え、また積極的に情報セキュリティ投資・対策のあり方について議論していく[9]。これは、情報セキュリティ事故

---

[5] マルウェアは、クラックツールやコンピュータウィルス、ワーム、スパイウェアに（悪質な）アドウェアなどと非常に広い範囲を含んでおり、「悪」を意味する接頭詞の “mal” をソフトウェア全般を意味する “ware” を繋げた比較的新しい造語である。

[6] http://www.ipa.or.jp/を参照されたい。

[7] 独立行政法人情報処理推進機構 (2002) によれば情報セキュリティとは、正当な権利を持つ個人や組織が、情報やシステムを意図通りに制御できる性質であると定義されている。そしてこの定義は、機密性、一貫性と可用性といった性質が満たされることを条件としている。それゆえに、情報セキュリティ被害とは、上記の性質が満たされないことを意味する。
なお、これらの情報セキュリティの目的については第2節を参照されたい。

[8] 例えば、竹村 (2006b) は、日本のインターネット・サービス・プロバイダ（ISP; Internet Service Provider）を対象にしたアンケート調査の結果から、多くのISPが情報セキュリティ対策の重要性は認識しているものの、費用対効果の観点から十分な情報セキュリティ対策を施せていないということを明らかにしている。

[9] もちろん、不正アクセスや攻撃のためのコストを高めることで、脅威を抑止するという動機付けも考えられるが、そ

は高度に情報化されたシステムの導入よりもそれを管理・運用、また利用している企業の行動に起因することが多く、これらを工学的に議論するのではなく経済学的に議論する必要があると考えたためである。この分野は萌芽の域を超えていないものの、第3節で見るように経済理論やゲーム理論を用いた研究や、アンケート調査などを通じて収集されたデータを用いた実証研究が進められている。

本稿の構成は以下の通りである。次節にて情報セキュリティの定義および近年におけるインターネットの脅威について説明を与える。第3節では経済学の側面から情報セキュリティを考えた理論研究と実証研究のサーベイを、また第4節では簡単に日本における情報セキュリティ対策・投資の現状について説明を与える。第5節では、情報セキュリティ投資を事業継続性の概念を用いて企業価値と関連付けることについて議論している。そして、最後の節にて、本稿のまとめと今後の展望について議論をおこなう。

2 情報セキュリティ

2.1 定義

本稿では、情報セキュリティとは「所有するサーバやコンピュータ、情報を様々な脅威から防護するための管理システム手の導入や、情報システムによって蓄積・作成された情報を健全かつ正確に運用管理すること」と定義する。

一般的に、情報セキュリティは図2のようにサブカテゴリーを持つとされている。

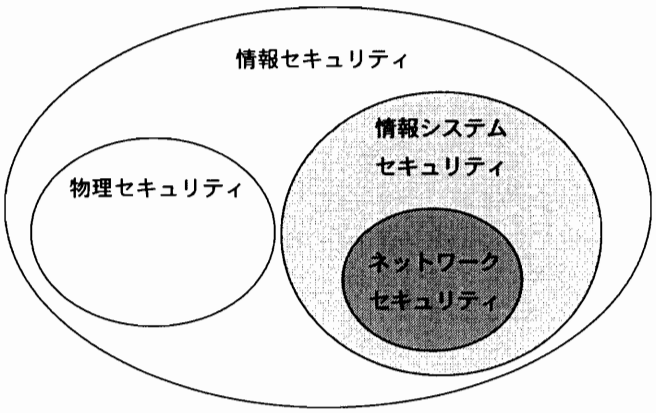


図 2: 情報セキュリティの概念図

れについては別論文として扱う。

物理セキュリティ 火災や地震などの自然災害や空巣などの犯罪から、建物や設備自体を保護するために施すセキュリティである。その対策として、建物自体やサーバ室などへの入退出管理や施錠などがある。

情報システムセキュリティ 企業をはじめとする様々な組織において作成・蓄積された情報を保護するための施すセキュリティである。その対策としては、製品を用いた技術的な対策（ファイアウォール、認証や暗号化、アンチウィルスなど）や、内部や外部ネットワークを適切に運用管理することなどがある[10]。

情報セキュリティは情報資産の分類と、それに基づく運用全般を指しており、その対象は、かなり広いものとなっている。そこで、本稿では、主として、情報システムセキュリティを対象に議論を進めていく。

研究動向や現状を議論する前に、簡単に情報セキュリティの目的とその機能について説明を与える。

2.1.1 情報セキュリティの目的

情報セキュリティの目的は、一般的に機密性（Confidentiality）、一貫性（Integrity）と可用性（Availability）であるとされている[11]。機密性とはアクセス権を持つものだけが、情報にアクセスできることを確実にすること、また一貫性とは情報およびその処理方法が正確であるだけでなく完全であることを保証することを意味している。そして、可用性とは許可されたユーザが必要なときに、情報及び関連する資産にアクセスできることを確実にすることを意味している。さらに、ICT社会の進展を受けて、本人認証（Athenticity）、責任・監査（Accountability）、道徳性（Morality）およびプライバシー（Privacy）などを考慮することもある[12]。特に、個人情報の保護に関する法律（個人情報保護法）などの成立によりプライバシーが近年重要視されるようになっている。

2.1.2 情報セキュリティの機能

情報セキュリティの機能をまとめたものが表1である。

いずれの機能もあらゆる組織にとって必須であり、重要なものである。特に、近年注目されている事業継続性（Business Continuity）の観点から、導入または運用管理している情報セキュリティ

---

10) 製品を用いた技術的な対策については竹村 (2006b, 2006c) などを参照されたい。

11) これらを合わせて、(情報) セキュリティの CIA と呼ばれることがある。

12) 本人認証と責任・監査、道徳性、プライバシーは、情報の作成者や送信者が本物であることを保証できること、システムがいつ、だれに利用されたかを追跡できること、正しいアクセスをおこなうこと、情報や提供サービスの利用が他者に観察されないようにすることをそれぞれ意味している。

表 1: 情報セキュリティの機能

機能	内容
抑制	情報セキュリティの存在が犯罪・事故・障害などを牽制・抑止する。
予防	情報セキュリティの存在が様々な脅威の顕在化や拡大を防止する。
検知	情報セキュリティの存在が事故・障害などを速やかに発見・通知する。
回復	情報セキュリティの存在が事故・障害などから正常な状態に回復する。

システムの定期的なチェック（情報システム監査や情報セキュリティ監査など）が必要であることは明らかである[13]。特に、重要インフラにおいては早急な回復機能が必要とされる[14]。

2.2 インターネットの脅威

インターネットの脅威は、発生している事件を鳥瞰すると、2つにカテゴライズされる。一つは、人間の欲望や実態無の無視、未熟さといったものでこれはWinny事件や情報紛失・漏洩に代表されるものである。もう一つは、近年急増している金銭目的のネット犯罪である。そしてこのネット犯罪の手口は、分業化、専業化している。特に不正アクセスインフラ（不正アクセスツールや不正接続サービスなど）、ブラック・グレーマーケット（闇市場）の存在がこれを可能にしているといえる。もともとコンピュータウィルスなどは作者の売名、いたずら（愉快犯）といったものが多かったが、近年ではその多くが金銭目的となっている。また、近年のインターネットの脅威の傾向として、ターゲットを特定化した攻撃（ターゲットアタック）や、何度も感染したりするダウンローダというものがある。昨今のインターネットの脅威をまとめたものが表2である。

インターネットの脅威をまとめたものが表3と表4になる。なお、用語説明には、IT用語辞典（http://e-words.jp）を用いた。

インターネットの脅威の変化は、攻撃者の目的の変化および緻密な制御ができるようになった結果、マルウェアの活動が見えにくくなってきている。従来のコンピュータウィルスやワークは広域に拡散しようとし、また駆除されるまでに感染活動を継続していたため定点観測データに表れやす

13) 事業継続性とは、地震、水害などの自然災害による施設の損壊、停電、人為的な障害、ハードウェア、ソフトウェアやネットワークの障害から情報システムを守り、サーバーやOSのアップグレード、ファイルのオンライン・バックアップなどの保守運用業務を行いながら、一定の条件の下で、情報システムを正常に稼働させ、付託された事業上の機能を保証することをいう。

14) 高度情報通信ネットワーク社会推進戦略本部 (2005) によれば、重要インフラとは、「他に代替することが著しく困難なサービスを提供する事業が形成する国民生活及び社会経済活動の基盤であり、その機能が停止、低下、または利用不可能な状況に陥った場合に、我が国の国民生活または社会経済活動に多大なる影響を及ぼすおそれが生じるもの」をいう。重要インフラ分野としては、情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービス（地方公共団体を含む）、医療、水道および物流がある。

表 2: インターネットの脅威の変化

	以前	近年
目的	愉快犯	犯罪・秘密暴露・金銭
経路	電子メール	ウェブ・電子メール・IM など
侵入方法	単純かつ一度	複数かつ連続 真の目的が不明
攻撃対象	不特定多数	特定の属性を持つ組織・人など

表 3: インターネットの脅威

種類	内容
コンピュータウィルス・ワーム	前者は他人のコンピュータに勝手に入り込んで悪さをするプログラムのことをいう。また、後者は自己増殖を繰り返しながら破壊活動をおこなうプロ　ラムのことをいう。
トロイの木馬	招待を偽ってコンピュータへ侵入し、データ消去やファイルの外部流出、他のコンピュータの攻撃などの破壊活動をおこなうプログラムのことをいう。
スパイウェア	パソコンユーザの行動や個人情報などを収集したり、マイクロプロセッサの空き時間を借用して計算をおこなったりするアプリケーションソフトのことを総称したものである。
フィッシング	正規のメールやウェブサイトを装い、暗証番号やクレジットカード番号などを搾取する詐欺のことをいう。
ファーミング	有名な金融機関やオンラインショップのサイトをそっくりにまねた偽のサイトを作り、DNS サーバの情報を書き換えることでユーザを誘導し、暗証番号やクレジットカード番号などを搾取することをいう。
ビッシング	IP 電話などに利用されている技術 VoIP を利用したフィッシング詐欺のことをいう。
ピギーバッグ	別のユーザによる正規の通信接続が無い時間にシステムに対するアクセス権限を得る行為（積極的な回線盗聴）をいう。

表 4: インターネットの脅威（続き）

種類	内容
spam・spim・spit	spam とは営利目的のメールを無差別に大量発信するもので、spim はインスタントメッセンジャー（IM; Instant Messenger）のユーザに向かって営利目的のメッセージを無差別に大量配信することをいう。また、spit とは IP 電話のユーザに向かって営利目的のメッセージを無差別に大量配信することをいう。
ボット・ボットネット	ウィルスなどによって多くのパソコンやサーバに遠隔操作できる攻撃用プログラム（ボット）といい、それをを送り込み、外部からの指令で一斉に攻撃を行なわせるネットワークのことをいう。
エビルツイン	偽アクセスポイントを随所に設置して強制的にフィッシングサイトに誘導するというものをいう。
ルートキット	クラッカーが遠隔地のコンピュータに不正に侵入した後に利用するソフトウェアをまとめたパッケージのことをいう。
ソーシャルエンジニアリング	ネットワークの管理や利用者などから、話術や盗み聞き、盗み見などの「社会的」な手段によって、パスワードなどのセキュリティ上重要な情報を入手することをいう。
ゼロディアタック	ソフトウェアにセキュリティ上の脆弱性（セキュリティホール）が発見されたときに、問題の存在自体が広く公表される前にその脆弱性を悪用して行なわれる攻撃のことをいう。
ワンクリック詐欺	不当料金請求の手法の一つで、アダルトサイトや出会い系サイトなどにパソコンや携帯電話からアクセスすると、いきなり料金請求の画面が表示される手口のことをいう。
ダウンローダ	リモート Web サイトからファイルをダウンロードして実行するように設計されており、一旦インストールされると、後日ウィルスなどが勝手にダウンロードおよび実行することができるプログラムである。

かったものの、ボットの場合は広域に拡散する必要がなく、攻撃者からの指示で即起動、停止が可能となり定点観測データに表れにくくなってきている[15]。

これらの状況を鑑みて、2006年12月に総務省と経済産業省が連携したサイバークリーンセンター（CCC, Cyber Clean Center）が発足し、ボットネット撲滅のための取組みが行われている[16]。

3 経済学における情報セキュリティの研究

高度情報化社会において情報セキュリティと経済学にまたがる文理融合型の学際的研究が必要とされている。言い換えると、社会や経済において十分な情報セキュリティを確保するためには、情報セキュリティ技術のみならず、それを管理・運用、また利用している企業の行動までを考慮した総合的な研究が必要なのである。

工学の分野では公開鍵などの情報セキュリティ技術に関する研究の蓄積が進んでいるが、その経済効果まで考えるものは少ない。また一方で、経済学の分野でもICT投資に関する研究は積極的におこなわれているが、情報セキュリティ技術を対象とした研究はほとんどなかった。

しかしながら、21世紀の到来とともに、この分野の学際的な研究が進められて、その成果が報告されている。以下、その主要な経済学的な研究を理論研究と実証研究に大別して紹介していく。

3.1 理論研究

経済学の分野における情報セキュリティの先駆的研究として、Gordon and Loeb (2002) とVarian (2002) がある。

Gordon and Loeb (2002, 2004) は企業行動の理論にたち、情報セキュリティ投資の経済効果を理論的に分析している。そして、脆弱性の水準と情報セキュリティ投資水準の関係を明らかにしている。また、松浦 (2003) は、Gordon and Loeb (2002) のモデルに保険を導入して最適な情報セキュリティ投資水準について議論を展開している。また、Gordon, Loeb and Lycyshyn (2003)、Gordon and Loeb (2003) やGordon and Loeb (2006) はGordon and Loeb (2002) をゲーム理論のフレームワークでもってモデルの再構築をおこなっている。

Varian (2002, 2004) は情報セキュリティをゲーム理論のフレームワークでもって理論的に研究している。そして、そこで情報システム全体を公共財としてとらえて、ただ乗り（free rider）の問題について議論している。また、Kunreuther and Heal (2003) はセキュリティの相互依存性につ

[15] 攻撃者が出す命令の例として、脆弱性などを狙った感染活動、機密情報（コンピュータ内の価値ある情報）の搾取、指定サーバに対するパスワード総当り攻撃やDDoS攻撃、サーバソフト（HTTPやFTPなど）の起動、スニッフィング（盗聴行為）、迷惑メールの送信や中継、スパイウェア等の不正インストールなどがある。これらを見ても分かるように、ボットネットの存在はインターネットの脅威を拡大させている一因になっている。

[16] CCCについては、https://www.ccc.go.jp/を参照されたい。

いて飛行機の荷物チェックを例に議論を展開している。そして、情報資産を保全する費用が正であれば、情報セキュリティ投資をおこなうことが絶対優位の戦略にはなりえないことを示している。

3.2 実証研究

田中 (2005) は情報処理実態調査の個票データを用いて、いくつかの情報セキュリティ指標を作成し、分析をおこなっている。そして、効果的な情報セキュリティ投資をおこなう上で、単に情報セキュリティシステムの導入にとどめるのではなく、組織管理や人材育成における対策を同時におこなう必要性を主張している。これは竹村 (2006, 2007) や本稿の主張とも一致したものとなっている。また、中程度の脆弱性レベルの情報システムにセキュリティ投資をおこなうことが合理的になることも明らかにしている。同様に、Gordon and Loeb (2002) のフレームワークと（総務省による）日本における e-ローカル・ガバメント（e-local govenment）のデータをもとに脆弱性と情報セキュリティ投資の関係を実証的に分析している Tanaka, Matsuura and Sudoh (2005) においても主張されている。

田中・松浦 (2006) は情報セキュリティ投資の経済的動機付けに関する研究調査をおこなっている。そしてその理論的フレームワークとして Gordon and Loeb (2002) を用いて、そのモデルの妥当政党についての検証も合わせておこなっている。その結果、ネットワークの脆弱性が中程度の部分にセキュリティ投資をおこなうことが効果的である可能性があること、またセキュリティ投資を行うに当たっては、ファイアーウォール等のハードウェアやセキュリティ対策アプリケーション等のソフトウェアに対策をとどめるのではなく、セキュリティ・マネジメントや人材教育などのいわゆる「目に見えない資産」への投資が重要なことを指摘している。さらに、セキュリティ対策を講じている企業に対しては、株式市場は目に見えない資産への投資を含めて積極的に評価し、企業価値が高くなる可能性があることについても示唆している。この第 3 の主張は本稿と一致した見解である。

情報通信インフラにおける情報セキュリティ対策について分析しているものとして、竹村 (2006c, 2007) や Ebara, Nakaniwa, Takemura and Yokomi (2006) がある。これらは、情報通信業の中でもインターネット・サービス・プロバイダ（ISP; Internet Service Provider）を対象に独自に実施したアンケート調査の結果をもとにして、近年大きな問題となっている情報セキュリティ対策およびそれに対する政策について議論している。そのために 2005 年度に実施したアンケート調査から ISP の情報セキュリティ対策の現状を明らかにし、また情報セキュリティ対策と経営パフォーマンスの関係について相関分析している。分析の結果、多くの ISP が情報セキュリティ対策の重要性は認識しているものの、情報セキュリティ対策には多額の資金が必要になり、必ずしも十分な情報セキュリティ対策をおこなっていないということが明らかになった。とりわけ経営パフォーマンスの低い地方都市の地域系 ISP は必ずしも十分な情報セキュリティ対策が施せているとはいえないことを確認している。このことは他の産業、さらに日本経済全体にとって大きな打撃になる可能性を

否めないことを指摘している。また、同時に規制緩和と安全性のトレードオフの関係についても指摘している。そして、それらをふまえて、本稿では情報セキュリティ遵守を義務づけた情報セキュリティ政策について様々な提案をおこなっている。

一方で、インターネットの脅威による情報セキュリティ被害額の試算をおこなっている研究もいくつか存在している。

NPO 日本ネットワークセキュリティ協会 (2003, 2004, 2005, 2006) は、日本の情報セキュリティ被害についての情報を収集し、そこから情報漏洩による想定被害（想定損害賠償額）を算出している。

Ferris Research (2003) は企業組織に与える spam メールのインパクトについて分析をおこなっている。そして、2002 年に米国で年間 89 億ドル、欧州で年間 25 億ドルの spam メールによる経済損失があったと試算している。また、Nucleus research (2004) によると米国企業が spam メールで被る労働生産性の割合は 1.4%になり、従業員一人あたりの spam メールを処理するための費用が年間 1934 ドルにものぼると試算している。同様に、Rockbridge Associates (2005) では米国を対象とした分析において、spam メールによって生じる労働損失額が 216 億円になるという試算を示している。

Rockbridge Associates (2005) にならい、榎原・鵜飼・竹村 (2005) と榎原 (2006) は日本における spam メールによって生じる労働損失額および過剰に必要とされているコンピュータ資本額を算出している。その結果、2004 年には spam メールによって生じている損失額は、前者が 170 億円、後者が 220 億円になると試算している。そして、これらの研究を受けて、Ukai and Takemura (2007) と Takemura and Ebara (2007) では、経済学的のフレームワーク（生産関数アプローチ）によって、spam メールによって生じる国内総生産（GDP; Gross Domestic Product）の損失額の推計およびシミュレーションをおこなっている。その結果、2004 年において spam メールによって生じる日本の GDP 額は約 5000 億円となり、また簡単なシミュレーションによると、spam メール対策が現状のままであれば 2010 年までに GDP の 1%にその損失額が達すると試算している。

これらの研究は、インターネット上の脅威が個人や企業などの組織、国など様々な主体に負の影響（莫大な経済損失）を与えており、情報セキュリティ対策が政策としても考えていく必要があることを示唆している。今後も、このようなインターネットの負の経済効果の測定に着目した実証研究の蓄積が必要とされる。そのためのデータベースの整備も必須である。

4 日本における情報セキュリティ対策・投資の現状

インターネットで種々のサービスを提供するサイトが攻撃されれば、（ネットワークの障害や負荷などを含む）被害は相当広範囲に及び、また被害額も高額になることが予想される[17]。情報

[17] 例えば、Yahoo!、CNN や Amazon.com などの米国大手商用サイトが 2000 年 2 月に DDoS（Distributed Denial of Service, 分散型サービス不能）攻撃を受けたとき、一時的に業務停止状態になった。また、その時の被害額は 12 億ド

セキュリティ被害は最悪のケースを考えると、経済全体に直接的もしくは間接的に波及してしまう可能性がある。これらの問題への対応として、米国や韓国の重要インフラを対象とした ISAC (Information Sharing and Analysis Center) に倣い日本では 2002 年 7 月に情報通信業を対象とし　Telecom ISAC Japan が設立され、情報セキュリティ対策に関する情報共有や各種インシデントの分析がおこなわれている[18]。銀行業においては、金融情報システムセンター (FISC; the Center for Financial Industry Information Systems) が重要な役割を果たして、それはうまく機能しているといわれている[19]。今後、他の (重要) インフラに関しても同様に、情報セキュリティ対策に関する組織の設置や運営が行われることが期待される。

また、政府も 2005 年 4 月に内閣官房情報セキュリティセンター (NISC; National Information Security Center) を設置して、Telecom-ISAC Japan や IPA などと連携をとりながら、情報セキュリティ対策に力を入れている[20]。しかしながら、現実問題として内閣官房・総務省・経済産業省 (2005) の指摘や竹村 (2006c, 2007) によれば、全体的なルールは決まったものの、現時点で必ずしもこれらがまだうまく機能しているとはいいがたい。ただ、第 2 節で説明したボットネットワーク撲滅のために設置された CCC についてはまだ設置されて間もないものの、その効果が出ていると報告されている。

たとえば、竹村 (2007) によれば、情報通信インフラにおいて必ずしも十分な情報セキュリティ対策が施されていないということが指摘されている。そして、現状のままにしておくことは日本全体おける情報セキュリティのレベルを引き下げることになると警鐘を鳴らしている。一般的に、企業や、産業、さらに国の情報セキュリティレベルというものは平均値ではなく、最も弱いところで測られる。それゆえに、この現状を改善するために、国や地方自治体もまた情報セキュリティ政策を考える必要があると主張している。

他の産業と同様に、情報通信業はほぼ自由に市場への参入や市場からの退出が可能となっている。これは経済学的には望ましい状況であるが、一方で「安全性」の面からとらえると必ずしもそうとはいえない。つまり、ビジネスチャンスが多いこの市場に多くの企業が利潤追求のみを目的として参入してきた場合、現状よりもさらに情報セキュリティのレベルが低くなる危険性がある。このことを考慮すると、情報通信業においては参入規制に一定の情報セキュリティレベル確保という条件を盛り込む必要性があるといえる。これは、規制緩和の流れに逆行するものではなく、近年いくつかの産業で問題になっている規制緩和と安全性のトレードオフを認識して政策立案をおこなわなければならないと主張するものである[21]。

ル以上になると米国の調査会社によって試算されている。

[18] Telecom ISAC は財団法人日本データ通信協会に編入されている。

[19] Nagaoka, Ukai and Takemura (2005b) を参照されたい。

[20] 2000 年 1 月に IT 戦略本部の設立とともに、内閣官房情報セキュリティ対策推進室が設置された。2005 年 4 月にこの対策推進室は 2005 年 4 月に内閣官房情報セキュリティセンターに改組された。

[21] 市場のルールを整備しないまま規制緩和をおこなった場合、様々な弊害が出るという批判がある。特に、費用便益の観点から安全性の優先順位が低くなることが挙げられる。

5　情報セキュリティ投資・企業価値・事業継続性

第3節で見たように情報セキュリティ投資を扱った研究の蓄積が進んでいる。しかしながら、まだその数は少ない。本節では、著者の過去におこなったアンケート・インタビュー・ヒアリング調査の結果および知見をもとに新たな情報セキュリティ投資に関するモデル構築の可能性について議論したい。

情報セキュリティ投資がなかなかおこなわれない理由として、費用対効果が不明確であることが多くの研究で指摘されている。第2節でみたようにインターネットの脅威は日々刻々と進化しており、その対策のための投資（特に、ソフトウェア投資やハードウェア投資）は多額となる一方で、本来の事業にて十分な収益をあげている企業はそれほど多くはない。そのために、情報セキュリティ対策は情報セキュリティ事故・被害が生じてからの事後対策となることが多い[22]。このことからも、情報セキュリティ投資が、他の投資と性質を異にしていることがわかる。つまり、既存の投資の関する経済モデルにおいて情報セキュリティ投資の経済効果をとらえることが難しい。そこで、様々なインタビュー・ヒアリング調査からの知見をICT投資の経済モデルに反映したモデル構築についての示唆を与えたい。第3節で見た田中 (2005) や田中・松浦 (2006) は Brynjolfsson, Hitt an Yang (2002) の Tobin's Q 理論を用いたモデルにおけるインタンジブルアセットを情報セキュリティ資産としてとらえている。これは、情報セキュリティ投資が企業の価値と関連していることを意味しており、従来のように情報セキュリティは費用を増大させるだけで必ずしも企業価値の向上などに反映されないという主張とは異なった見解である[23]。

本稿では、彼らと同様に情報セキュリティ投資が企業価値向上と関連があるという仮説を支持する。この仮説が検証され、その妥当性が認められれば、各企業が情報セキュリティ投資を積極的におこなわせる論拠（情報セキュリティ投資をおこなうインセンティブ）となりうる。つまり、情報セキュリティ対策の費用対効果を明確にし、正の経済効果が存在することを示すことにより、積極的に情報セキュリティ対策がおこなわれ、同時にある一定以上の情報セキュリティレベルが確保されることを意味する。この仮説の根幹を支えているものは近年注目されている「事業継続性」の概念である。最後に、この事業継続性と企業価値、情報セキュリティ投資の関係について簡単に論じる。

それゆえに、情報セキュリティ事故などが起こり、情報セキュリティ対策が十分にできていないために、事後対策が不適切となれば（もちろん事前対策についても同様である）、企業は市場での評価（企業価値）が下がり、予想以上の損害・ダメージ（たとえば、社会的信頼の失墜など）を被るかもしれない。それを回避するためにも情報セキュリティ対策・投資が必要となるのである。この意味において、情報セキュリティ対策・投資は単なる形式的なものではなく、戦略的なものであ

[22] 著者がIPSを対象におこなったインタビュー・ヒアリング調査においてもこの種の意見がよせられている。また、2007年2月にISPを対象に実施した情報セキュリティと対策のアンケートやインタビュー・ヒアリング調査の結果についても近日中に集計をおこない、まとめる予定である。

[23] 独自におこなったインタビュー調査などによれば、業務に制約がかけられるために、生産性を低下させるという意見もあった。

る必要がある。なお、この戦略的情報セキュリティ投資に関する理論モデルについては、2007年2月に実施しているアンケートデータを用いて、別論文にて扱う予定である。

6 おわりに

情報セキュリティを考慮した様々な政策において、情報セキュリティレベルの基準設定を考えなければならない。重要インフラ、特に情報通信インフラにおける情報セキュリティのレベルは高く設定されるべきである。この基準設定に関して、地域間で異なってはいけない。そのために、情報セキュリティに関してコーディネートする存在および法制度の整備・充実が必要である。2005年4月に設置されたNISCは、産業・省庁を横断する情報セキュリティに関するコーディネーターとしての役割を担っている。現在、NISCは他の組織と連携しながら、日本の情報セキュリティに関する研究や基準設定などをおこなっている[24]。なお、その活動はホームページにて報告されている[25]。もちろん、これらの組織がコーディネートしても、それを個人や企業が従わなければ意味がない。情報セキュリティ対策は、ネットワークを利用している全ユーザが施さなければならない義務なのである。また、情報セキュリティに関する法整備についても国内外の研究を踏まえながら早急に進めていかなければならない。

重要な問題について指摘して本節を終わることにする。それは情報セキュリティ政策を実施する際、竹村 (2006c, 2007) でも指摘されているように、規制緩和と安全性のトレードオフを考慮する必要があるといったことである。市場のルールを整備しないまま規制緩和をおこなった場合、様々な弊害が出て、費用便益の観点から安全性の優先順位が低くなってしまう。そのために、トレードオフを認識して政策立案をおこなわなければならない。

本稿では、近年社会問題化し、また喫緊かつ重要な課題となっている情報セキュリティ対策、とりわけ重要インフラにおけるその対策について議論した。これはIT投資の中でも情報セキュリティ投資が性質を異しているために、既存のフレームワークで必ずしもとらえられるとは限らないことを指摘した。それは、情報セキュリティ投資という新たなIT投資を組み込んだ経済モデルを構築する必要があることを意味している。その一つが。第5節の最後で簡単に提示した事業継続性に関連した企業価値モデルである。

また同時に、生産性を向上させるためだけのIT投資ではなく、インフラとしての役割を果たすためにも、自らがもつ情報システムを防護するための投資が必要であるということについて主張した。情報セキュリティ投資は、IT投資に関する研究を深化させたもののひとつである。つまり、これは新たなIT投資の研究の対象であり、その意義は大きいといえる。特に、情報セキュリティ投資を研究する場合は、国レベルや産業レベルではなく企業レベルの研究である必要がある。それは、集計されたデータでは、情報セキュリティへ投資している企業とそうでない企業を集計して一

[24] NISCの取り組みについては、内閣官房情報セキュリティセンター (2006) などが詳しいので参照されたい。
[25] http://www.bits.go.jp/（2007年2月現在）

緒にしてしまうために、その経済効果が消えてしまう可能性がある[26]。そのためにも、企業レベルのデータセットの構築も急速に望まれる。

参考文献

[1] Brynjolfsson, E., L. Hitt and S. Yang (2002), "Intangible Assets: How the Interaction of Computers and Organizational Structure Affects Stock Market Valuations," *Brookings Papers on Economic Activity: Macroeconomics* Vol.1, pp.137-199.

[2] Ebara, H., A. Nakaniwa, T. Takemura and M. Yokomi (2006), "Empirical Analysis of Internet Service Provider and Its Policy Implications," *RCSS Discussion Paper Series*（関西大学ソシオネットワーク戦略研究センター）, No.42.

[3] Ferris Research (2003), "Spam Control: Problems and Opportunities," Ferris Research, Inc.

[4] Gordon, L. A. and M. P. Loeb. (2002) "The Economics of Information Security Investment," *ACM Transactions on Information and System Security*, Vol.5, pp.438-457.

[5] Gordon, L. A. and M. P. Loeb. (2004) "The Economics of Information Security Investment," Camp, L. J. and S. Lewis eds., *The Economics of Information Security (Advances in Information Security)*, pp.105-127.

[6] Gordon, L. A. and M. P. Loeb (2006), "Expenditures on Competitor Analysis and Information Security: A Managerial Accounting Perspective," Bhimni, A. ed., *Management Accounting in the Digital Economy*, pp.95-111.

[7] Gordon, L. A. and M. P. Loeb (2006), *Managing Cyber-Security Resources: A Cost-Benefit Analysis*, the McGraw-Hill Companies.

[8] Gordon, L. A., M. P. Loeb and W. Lucyshyn (2003), "Sharing Information on Computer Systems Security: An Economic Analysis," *Journal of Accounting and Public Policy*, Vol.22(6), pp.461-485.

[9] Kunreuther, H. and G. Heal (2003), "Interdependent Security," *The Journal of Risk and Uncertainty*, Vol.26, pp.231-249.

[10] Nucleus Research (2004), "Spam: The Serial ROI Killer," *RESEARCH NOTE*, **E50**.

[26] この主張は、技術革新相殺効果に似ているといえる。

[11] Rockbridge Associates (2005), "2004 National Technology Readiness Survey: Summary Report," Rockbridge Associates, Inc.

[12] Takemura, T. and H. Ebara (2007), "An Economic Model of Spam Mail," *Mimeo*, Kansai University, http://www.rcss.kansai-u.ac.jp/takemura/.

[13] Tanaka, H., 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*, Vol.24 (1), pp.37-59.

[14] Ukai, Y. and T. Takemura (2007), "Spam Mail Damages Economic Growth," *The Review of Socionetwork Strategies*, Vol.1, pp.14-22.

[15] Varian, H. R. (2002), "System Reliability and Free Riding," *ACM Transactions on Information and System Security*, Vol.5, pp.355-366.

[16] Varian, H. R. (2004), "System Reliability and Free Riding," Camp, L. J. and S. Lewis eds., *The Economics of Information Security (Advances in Information Security)*, pp.1-15.

[17] 江良亮・竹村敏彦 (2005),『電気通信インフラ整備と政策評価（平成 16 年度自主研究報告書)』（国際通信経済研究所）, RITE04-J04, pp.1-41.

[18] 榎原博之 (2006),「spam メールによる経済損失: ISP の重要課題」榎原博之・中庭明子・竹村敏彦・横見宗樹『インターネット・サービス・プロバイダの実証分析』多賀出版, pp.177-190.

[19] 榎原博之・鵜飼康東・竹村敏彦 (2005),「spam メールの経済的損失の試算」RCSS ディスカッションペーパー（関西大学ソシオネットワーク戦略研究センター）, 第 33 号.

[20] 高度情報通信ネットワーク社会推進戦略本部 (2005),『第 2 次提言 我が国の重要インフラにおける情報セキュリティ対策の強化に向けて』http://www.bits.go.jp/.

[21] 総務省 (2002),『情報通信白書』ぎょうせい.

[22] 総務省 (2005),『情報通信白書』ぎょうせい.

[23] 総務省 (2006),『情報通信白書』ぎょうせい.

[24] 竹村敏彦 (2006a)「日本における IT 投資の経済効果－銀行業を中心とした企業レベルデータからの検証－」大阪大学博士（応用経済学）学位取得論文.

[25] 竹村敏彦 (2006b),「インターネット・サービス・プロバイダの情報セキュリティ対策とその実態」榎原博之・中庭明子・竹村敏彦・横見宗樹『インターネット・サービス・プロバイダの実証分析』多賀出版, pp.149-175.

[26] 竹村敏彦 (2006c),「情報通信インフラにおける情報セキュリティ政策の提案ーアンケートデータを用いた分析からの考察ー」RCSS ディスカッションペーパー（関西大学ソシオネットワーク戦略研究センター）, 第 40 号.

[27] 竹村敏彦 (2007),「情報通信インフラにおける情報セキュリティ政策の提案」村田忠彦・渡邊真治 編『ソシオネットワーク戦略とは何か』多賀出版, *forthcoming.*

[28] 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」『情報学研究』（東京大学大学院情報学研究科）No.69, pp.123-136.

[29] 田中秀幸・松浦幹太 (2006),「情報セキュリティ投資の経済的動機付けに関する企業レベルの実証研究」, 研究調査報告書（財団法人電気通信普及財団）, 第 21 号, pp.9-16.

[30] 独立行政法人情報処理推進機構 (2002),『情報セキュリティの現状ー 2001 年度ー』, ppI-1-I-29.

[31] 内閣官房情報セキュリティセンター (2006),「我が国政府の情報セキュリティ問題への取組みー内閣官房の取組みを中心としてー」『Network Security Forum 2006 カンファレンスノート』（ネットワークセキュリティフォーラム 2006）, pp.1-19.

[32] NPO 日本ネットワークセキュリティ協会 (2003),『2002 年度情報セキュリティインシデントに関する調査報告書: 情報セキュリティのインシデントに関する調査および被害算出モデル』

[33] NPO 日本ネットワークセキュリティ協会 (2004),『2003 年度情報セキュリティインシデントに関する調査報告書: 情報セキュリティのインシデントに関する調査および被害算出モデル』

[34] NPO 日本ネットワークセキュリティ協会 (2005),『2004 年度情報セキュリティインシデントに関する調査報告書: 情報漏えいによる被害想定と考察（賠償額および株価影響額）』

[35] NPO 日本ネットワークセキュリティ協会 (2006),『2005 年度情報セキュリティインシデントに関する調査報告書: 情報漏えいによる被害想定と考察（想定損害賠償額の算定）』

[36] 松浦幹太 (2003), “情報セキュリティと経済学,” 2003 年暗号と情報セキュリティ・シンポジウム（SCIS2003）予稿集, pp.475-480.

[37] 山口英 (2007),「学会への期待」JSSM セキュリティ公開討論会配布資料, http://www.jssm.net/.