RCSSディスカッションペーパーシリーズ
第40号　2006年6月

Discussion Paper Series
No.40 June, 2006

ISSN 1347-636X

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

— アンケートデータを用いた分析からの考察 —

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

情報通信インフラにおける
情報セキュリティ政策の提案

― アンケートデータを用いた分析からの考察 ―

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

情報通信インフラにおける情報セキュリティ政策の提案*

－アンケートデータを用いた分析からの考察－

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

2006年6月

概 要

本稿では、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（Internet Service Provider; 以下、ISPとする）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する。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を分析する。

この結果、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もわかった。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。

そこで、これらの結果をふまえて、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いくつかの提案をおこなっている。

KEYWORD: 情報通信インフラ, 情報セキュリティ, インターネット・サービス・プロバイダ, スピアマンの順位相関係数, 重要インフラ

*本稿の一部は、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、本論文は公益事業学会第56回大会での報告内容に大幅に加筆・修正を加えたものである。討論者の渡井理佳子氏（日本大学大学院法務研究科・助教授）および座長の安部誠治氏（関西大学商学部・教授）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。また、業務多忙のなか筆者らのアンケート調査およびインタビュー調査にご協力いただいたISP各社様に厚く御礼を申し上げたい。最後に、榎原博之（関西大学工学部・助教授）、横見宗樹（大阪商業大学・専任講師）、中庭明子（大阪産業大学・助手）および煩雑なデータ入力をお手伝いいただいた部奈和洋（大和住銀投信投資顧問会社業務管理部）の諸氏に感謝する次第である。

†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

Suggestions for Information Security Policy on Information and Communication Infrastructure
–Discussion from Analysis Using Questionnaire Data–

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

Abstract

In this paper, we focus on internet service providers (ISPs) and discuss ISPs' information security countermeasure and the policy by using results of questionnaire we conducted at 2005. For the purpose, we throw up the circumstances concerning information security countermeasures by using the results of questionnaire, and we analyze the relationship between degree of the information security countermeasures and management performance.

As the result, we found the following. Although Many ISPs recognize the importance of the information security countermeasures, adequate countermeasures are never taken. Especially local ISPs which are low performance, do not take adequate information security countermeasures. The existence of a part of ISPs taking inadequate security countermeasures reduces the level of the information security of not only the information and communication industries but also the whole country. In addition, we point out the trade-off between deregulation and safety (security).

In this paper, we suggest some information security policies toward the government to legislate information security compliance.

KEYWORD: Information and Communication Infrastracture, Information Security, Internet Service Provider, Spearman's Rank Correlation Coefficient, Critical Infrastructure

1 序論

インターネットが商用利用されるようになって10年以上経った。この間、インターネットは社会生活や企業活動にとって必須のツールとなり、また情報通信インフラと位置づけられるようになった。また、情報通信インフラは、電力、金融と並んで重要インフラの中でも重要視されている[1]。これは、2000年からのe-Japan戦略、さらにe-Japan戦略IIでとなえられていた高度情報通信ネットワーク社会の形成に適うものになりつつある[2]。また、これを具体化するe-Japan重点政策5分野の中に「高度情報通信ネットワークの安全性及び信頼性の確保」を挙げて、情報セキュリティ水準の向上を目指している。

しかしながら、近年コンピュータウィルスや不正アクセス[3]などによる情報セキュリティ被害という深刻な社会問題も顕在化してきている。近年、日本では官邸のホームページ改竄や企業においてウィルスに感染したP2P[4]（Peer-to-Pear）ファイル交換ソフトを通しての情報漏洩事故などが多数報告されている。情報セキュリティ検討会(2006)によれば、独立行政法人情報処理推進機構（Information-Technology Promotion Agency, Japan, IPA）に届出されたウィルス件数（54,174件）は5年間で約4.9倍まで増加し、また不正アクセスに関しては実際に被害にあった届出件数が前年に比べて約2.4倍に増加している。このように、現在では情報セキュリティ被害に遭遇する危険性が多分にある。

これらの状況を踏まえながら、個人も各企業も十分なセキュリティ対策を講じなければならない。もし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[5]。つまり、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てTelecom

---

[1] 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。従来、重要インフラ分野とされてきた情報通信、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）に加えて、2004年12月に開催された情報セキュリティ基本問題委員会第2分科会にて、新たに医療、水道と物流が付け加えられた。

[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、情報通信技術（ICT: Information and Communication Technology）の活用により世界的規模で生じている急激かつ大幅な社会経済構造の変化に適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関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（2006年8月現在）。

[3] 不正アクセスとは、コンピュータへの正規のアクセス権を持たない人が、システムの脆弱性やソフトウェアの不具合などを悪用してアクセス権を取得し、不正にコンピュータをアクセスすることをいう。代表的な不正アクセスには、セキュリティホールを悪用してファイルを盗み見たり削除・改変したりする行為や、盗聴や総当たり攻撃によるパスワード窃取、メールサーバを悪用した迷惑メールのばらまきなどがある。

不正アクセスによる被害はインターネットの普及と共に急増していることから、1999年に不正アクセス禁止法が成立して、これらの行為は犯罪行為として処罰されることになった。

[4] P2Pとは、不特定多数の個人間で直接情報のやり取りをおこなうインターネットの利用形態である。ここでは、WinMXやWinny、Napsterなどのファイル交換ソフトを使って、ある程度匿名的にファイル転送できる機能を持ったファイル共有ネットワークのことをいう。

[5] 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。

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[6]。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（National Information Security Center, NISC）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[7]。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2005年7月に実施したアンケートの結果によれば、現時点で必ずしもこれらがうまく機能しているとはいいがたい。

本稿では、情報通信インフラの中でも特に個人や企業を対象にインターネット・サービスを提供しているインターネット・サービス・プロバイダ（ISP: Internet Service Provider）に注目して分析をおこなっていく。ISP とは、電話回線や ISDN 回線、データ通信専用回線などを通じて、ユーザである個人や企業にインターネット環境を提供することを基本的な業務としている通信事業者のことをいう[8]。

本稿では、各 ISP がとるべき情報セキュリティ対策のみならず、国や地方自治体がとるべき情報セキュリティ政策のあり方について議論する。そのために、まず ISP の情報セキュリティ対策の現状の把握をおこなう。これには、2005年7月に社団法人日本インターネットプロバイダー協会のホームページ掲載されている ISP（593社）に郵送で記名方式のアンケート調査をおこなった結果を用いる[9]。次に、経営パフォーマンスと情報セキュリティ対策の関係を相関分析によって調べる。

ここで、簡単に先行研究について触れておくことにする。ISP を対象にした実証研究はまだ萌芽の域を超えていないために、先行研究に関しても横見・榎原・中庭・竹村 (2004)、横見・榎原・中庭・竹村・鵜飼 (2004)、竹村 (2006b)、横見 (2006) や峰滝 (2006) などとまだ数少ない。その主たる理由は、公表された個票データが存在しないことにある[10]。

本稿の構成は以下の通りである。まず、次節で ISP を取り巻く市場について考察し、第3節でアンケート調査に基づく ISP の情報セキュリティ対策の現状について述べる。次に、第4節では分析手法を提示すると同時に、その分析結果を示す。最後の節にて国や地方自治体がとるべき情報セキュリティ政策のあり方について提言をおこなうとともに、今後の課題について述べる。

2 ISP を取り巻く市場の変遷

本節では、ISP を取り巻く市場の変遷について考察をおこなう[11]。

---

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

[7] 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。

[8] この ISP の定義は狭義なものである。現在の ISP は、接続サービスの他にアプリケーションサービスなど、様々なサービス提供をおこなっている。

[9] 有効回答数は30社（有効回答率は約5.1%）であった。アンケートの回収率は約6.75%であった。なお、アンケート調査は匿名を条件にしているので、本稿では一切の企業名は公表しない。

[10] 峰滝 (2006) では特定サービス産業実態調査の個票データ、それ以外の研究ではアンケート調査から収集した個票データでもって分析をおこなっている。いずれも公表されたデータではなく、今後研究を深化させるためには、公表されたデータベースなどの構築が必要であると考える。

[11] たとえば、みずほコーポレート銀行産業調査部 (2002) は ISP の黎明期から近年までの状況に詳しいので参照されたい。また、提供しているサービスの種類や ISP の形態については竹村 (2006a) を参照されたい。

黎明期においてISPが提供する接続サービスはダイアルアップ接続が主流で、ユーザはウェブとE-mailの利用が主たる目的であった。そのため、各ISPは挙ってアクセスポイントを増設するといった戦略をとり、ユーザの確保を試みた。ICTの進展によって常時接続サービスが出現し、それと同時にビジネスチャンスを求めて多くの企業がこの市場へ参入してきた。また、少し時期をずらして通信キャリアやケーブルテレビ（CATV: Community Antenna TeleVision）が市場へ参入し、1990年代後半にISPの乱立期が訪れた。この時、各ISPが他のISPに対抗してユーザを確保するためには、接続サービスの低価格化（定額制を含む）をおこなうしかなかった。さらに2000年に入ってブロードバンド接続[12]の到来によって、低価格で高品質の接続サービスのみならず、種々のアプリケーションサービス[13]（IP電話、ブログ、コンテンツサービスなど）やオペレーションサービス[14]（ホスティングサービスやハウジングサービスなど）を提供しなければ、各ISPは市場で生き残っていくことが困難になっている。

実際に、これら全てのサービスを各ISPがユーザに提供できるわけではない。特に地方都市にある地域系ISPは地理的な条件などによってユーザの確保が難しく、また経営も悪化の一途を辿っている。その一因として、社団法人日本インターネットプロバイダー協会 (2003) や横見・榎原・中庭・竹村 (2004) で指摘されているようにバックボーンコストによる経営の圧迫が考えられる[15]。とりわけ、地域系ISPは地域密着の視点からインターネットを地域社会に普及させるとともに情報通信インフラの整備に大きく貢献してきたことを考慮すると、バックボーンコストのあり方について考えなければならない。なお、これについては第5節で議論する。

近年では、接続サービスを提供せずにアプリケーションサービスを企業などに提供する事業者であるアプリケーション・サービス・プロバイダ（ASP: Application Service Provider）が出現している。このようにアプリケーションサービスの提供に特化することによって、新たなビジネスモデルが生まれている。

一方で、インターネット上のトラヒックを分析した岡田・川原 (2003) や亀井・森・大井 (2003) は「P2Pトラヒックが全トラヒックの6割程度を占めている」という分析結果を得ている。これは、多額な投資をおこなって提供している様々なアプリケーションサービスがユーザにとって必ずしも魅力的なものとなっていないことを意味している。この意味においても、各ISPは今後提供するアプリケーションサービスを精査していく必要があるといえる。また、近年社会問題化しているP2Pの使用についても何らかの処置をとるようにしなければならない。

本節の残りで、ISPのユーザ（個人および企業）についても少し概観する。

図1には1997年から2005年にわたるインターネット利用者数の推移が示されている。1997年

---

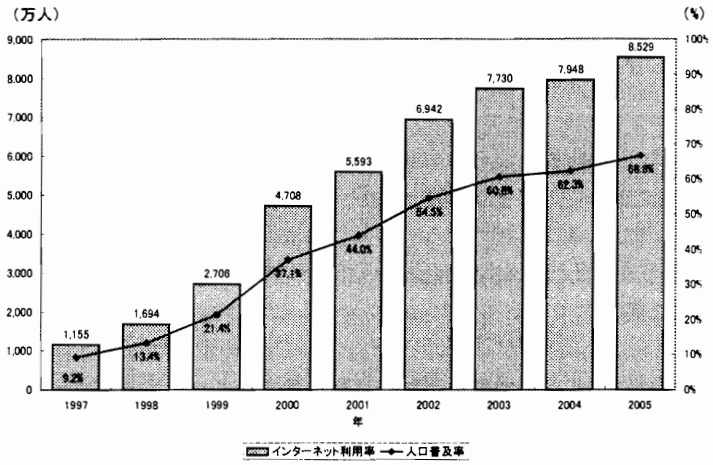
12) ブロードバンド接続サービスとはCATVやADSL、光ファイバなどの最近のICTを利用し低価格で高速な伝送速度の回線を提供するサービスのことをいう。ブロードバンド接続サービスの回線速度はベストエフォート型で提供されているため、回線速度の実効値は保障されない。このことを除いては、利用料金が一定であることから常時接続サービスとほとんど変わらない。

13) アプリケーションサービスとは、ISPのネットワークを構成するコンピュータのサーバアプリケーション機能に基づいて提供するサービスのことである。

14) オペレーションサービスとは、ネットワークに対する情報の設定、または装置からの情報取得をおこなうためのコンピュータ、または運用者により提供されるサービスをいう。

15) バックボーンコストとは、インターネット・サービス・プロバイダ内の接続拠点間を結ぶ回線や、プロバイダと他のプロバイダやIX（Internet eXchange）を結ぶ回線を所有している1次プロバイダに対して2次プロバイダが支払う利用料（接続料）のことである。ISPの黎明期に比べるとこのコストは大幅に下がったものの、依然として高い水準にある。

に 1,155 万人だったインターネット利用人口は 2005 年には 8,529 万人、また 9.2%だったインターネット人口普及率は 2005 年には 66.8%まで増加した。インターネットの利用用途としては、ショッピング、ニュースや天気予報などの情報収集、インターネットコンテンツ（音楽や動画など）、コミュニケーション（掲示板、ブログ、インスタントメッセンジャーやソーシャルネットワーキングサイトなど）、オンラインゲームなどが挙げられる。



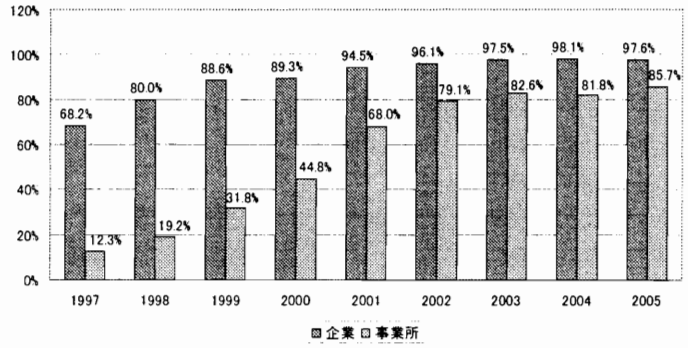
総務省 (2006) より作成

図 1: インターネット利用人口と人口普及率

図 2 を見てわかるように、1997 年において 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、ほぼ全ての企業でインターネットが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。企業の利用用途は大きく個人とは異なり、ASP や iDC[16] （internet Data Center）の利用、B2B や B2C などの新たなるビジネスチャンスを視野に入れたものとなっている。

これらのことからも、社会がインターネットに強く依存していることがわかる。言い換えると、現在の高度情報化社会において、インターネットは個人の生活や企業の経済活動に深く密着し、それと同時にインフラ（情報通信インフラ）として重要な役割を果たしている。

16) iDC とは顧客のサーバを預かり、インターネットへの接続回線や保守・運用サービスなどを提供する施設のことをいう。これは、ISP の提供しているオペレーションサービスの 1 つであるハウジングサービスに該当する。
インターネットビジネスでは、中核業務以外はアウトソーシングして組織を身軽にすることが競争力につながるため、インターネットの普及に伴ってデータセンターの需要はますます増大している。



総務省 (2002, 2005, 2006) より作成より作成

図 2: 企業・事業所のインターネット導入率

3 ISP の情報セキュリティ対策の現状

関西大学ソシオネットワーク戦略研究センターの「情報技術の統計解析研究会」[17] では、ISP の経営パフォーマンス定性的かつ定量的に研究をおこなっている。その一環として、ISP の情報セキュリティ対策の現状把握とともに、情報セキュリティ対策と経営パフォーマンスの関係を明らかにすることを目的として、2005 年 7 月時点で「社団法人日本インターネットプロバイダー協会」のホームページに掲載されている 593 社の ISP を対象に郵送で記名式のアンケート調査をおこなった。ここでは、このアンケート調査の結果から得られた ISP の情報セキュリティ対策の現状についてまとめる。

アンケートでは、大別して、情報セキュリティ対策などに関する質問、財務・サービスなどに関する質問、および政府の情報セキュリティ対策に関する質問がある。なお、詳細なアンケートの集計結果については、竹村 (2006b) を参照されたい。

直近 1 年間における情報セキュリティ被害にあった ISP の割合は約 39.2%であった。具体的な被害として、最も多かったのが DoS 攻撃[18]、続いてウィルス被害と不正アクセスであった[19]。被害後には、情報セキュリティシステムを導入したり、情報セキュリティ被害に関するコンティンジェンシープラン[20] を盛り込んだ情報セキュリティポリシーを策定したりといった対策を施している。このことからもわかるように、全ての ISP において情報セキュリティポリシーは策定されておく

[17] http://www.rcss.kansai-u.ac.jp/ISP/

[18] DoS (Denial of Service) 攻撃とは、インターネットのサーバなどをクラッキング (悪意を持って攻撃、破壊すること) する手法の 1 つで、各種サーバに対して大量の (無意味な) サービス接続要求を送りつけて、サーバの負荷を高めてサーバを過負荷でダウンさせたり、他の正当なユーザへのサービスを妨げたりする攻撃のことである。

[19] 被害にあった大半の ISP が「金銭的な被害ではなく、その他の被害が多々あった」と回答している。具体的には、トラブル対応などが挙げられる。

[20] コンティンジェンシープラン (contingency plan) とは、緊急時対応計画、危機管理計画や非常事態発生時対応計画などと訳され、事件・事故・災害などの不測の事態が発生することを想定し、その被害や損失を最小限にとどめるために、あらかじめ定めた対応策や行動手順のことである。

べきである。

アンケート調査の結果、どのISPも情報セキュリティ対策の重要性は認識しているものの、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が明らかになった。その理由として、現在の経営状態から情報セキュリティ対策が最優先されないこと、ISP自体が十分な技術や知識を必ずしも有していないことが挙げられている。また、1節で言及したようなTelecom ISAC Japanの存在について知らないISPも多く存在していた。

情報セキュリティ対策には多額の資金が必要であり、費用便益の関係でとらえた場合、情報セキュリティ対策よりも既存の提供しているサービスへの追加投資もしくは新規サービスのへの投資が優先されてしまう。また、従業員数が少ない地域系ISPは、必ずしも情報セキュリティに関する知識や技術を導入することが容易ではない。

しかしながら、これらの理由のため、情報通信インフラを担うISPが現状のままでいいということにはならない。一般的に、情報セキュリティ対策は一部の企業が対策を実施することで成しうるものでない。インターネットというネットワークによって社会全体がつながっていることを考慮すると、全ての企業や個人が完全な対策をしてこそ、効果的な情報セキュリティ対策が施せるといえる。特に、ISPの情報セキュリティ対策のレベルは他の企業よりも高く設定すべきであると考える。それは、情報セキュリティ対策に劣る一部のISPの存在が情報通信産業だけでなく、日本全体おける情報セキュリティのレベルを引き下げていることが懸念されるからである。

また、アンケートから情報セキュリティに関する法的な制度の確立をもとめる意見もあった。総務省や経済産業省から公表されているいくつものガイドラインがある中で、個人情報保護のように情報セキュリティの中の一部分を切り出したガイドラインが存在するなど、大変わかりにくい体系となっている。そのために国レベルで統一したガイドラインをつくる必要性がある。この意味においても、NISCの存在意義が今後大きくなることが予想される。

4 相関分析

ここでは、情報セキュリティ対策と各ISPの経営パフォーマンスの間に何らかの関係があるか否かについて分析をおこなう。これらを調べることによって、次節で議論するISPの経営戦略や、国や地方自治体がとるべき情報セキュリティ政策において必要となる情報を与えることができる。

4.1 分析手法

2変数間の関係を見る指標の1つとして、直線的な相関の程度を表す相関係数がある。通常、定量的な2変数間の相関関係は間隔尺度によって測られるピアソンの積率相関係数（Pearson's product-moment correlation coefficient）が用いられる[21]。しかしながら、間隔尺度でもって測られるデータであっても正規分布に従わない場合や、もともとデータが順序尺度である場合にこれらは利用できない。このような場合に利用できる相関係数として順位相関係数がある。なお、

[21] 間隔尺度とは、データの大小比較ができるという方向性、あるいはデータに順番をつけることができる順序性に加えて、個々のデータ間に間隔が保証されている尺度のことをいう。

アンケート調査によく用いられる順位相関係数として、スピアマンやケンドールの順位相関係数（Spearman's/Kendall's rank correlation coefficient）が有名である。

本稿では、スピアマンの順位相関係数を用いてセキュリティ対策と経営パフォーマンスの関係を調べる。以下、簡単にスピアマンの順位相関係数の導出手順を説明する。

変数 $X = (X_1, X_2, \ldots, X_i, \ldots, X_n)$ と変数 $Y = (Y_1, Y_2, \ldots, Y_i, \ldots, Y_n)$ についてそれぞれ小さい方から順位をつける。ただし、同順位には平均順位をつける。これらの変数の組 (X_i, Y_i) における順位差を d_i で定義して、順位の一致性の指標であるこの二乗和 $\sum d_i^2$ を求める。なお、2 変数の順位が完全に一致すればこの二乗和は 0 になり、完全に逆順となれば $(n^3 - n)/3$ になる。この性質を用いて、$-1 \leq r_s \leq 1$ となるように調整することで変数に同順位がある場合のスピアマンの順位相関係数 r_s を式 (1) によって計算することができる。

$$r_s = \frac{T_x + T_y - \sum d_i^2}{2\sqrt{T_x T_y}} \tag{1}$$

$$T_x = \frac{(n^3 - n) - \sum_{j=1}^{n_x}(t_j^3 - t_j)}{12}, \quad T_y = \frac{(n^3 - n) - \sum_{k=1}^{n_y}(t_k^3 - t_k)}{12}$$

n_x: 変数 X における同順位の個数
n_y: 変数 Y における同順位の個数
t_j: 変数 X における同順位の大きさ（$j = 1, 2, \ldots, n_x$）
t_k: 変数 Y における同順位の大きさ（$k = 1, 2, \ldots, n_y$）

$r_s > 0$ であれば変数 X と変数 Y に正の相関関係、また $r_s < 0$ であれば両者に負の相関関係があることになる。一方で、$r_s = 0$ であれば両者に全く相関関係が存在しないことになる。

続いて、この導出された順位相関係数が統計的に有意なものであるか否かを検定する。この検定における帰無仮説は「母相関係数はゼロである」、また対立仮説は「母相関係数はゼロではない」である。もし帰無仮説が棄却されれば、変数間に正もしくは負の相関関係が存在することを確認できる。詳細な検定方法については、芝・南風原 (1990) などを参照されたい。

4.2 データ

ここでは、分析に用いる変数の特定化およびそのデータの加工をおこなう。2005 年 7 月におこなったアンケート調査から収集したデータをもとに、情報セキュリティ対策の指標および経営パフォーマンスの指標を作成した。

分析に用いるデータ数は 30 社であり、その内訳は北海道（1 社）、東北（4 社）、北陸（3 社）、関東（8 社）、東海（3 社）、関西（5 社）、中国（2 社）、四国（2 社）、九州（2 社）となっている。また、以下の分析で用いるデータは全て 2004 年度時点のものである。

情報セキュリティ対策の指標（順序尺度）として、情報セキュリティ対策の優先順位、情報セキュリティ教育実施の程度、情報セキュリティシステムの導入数（種類）、情報セキュリティ対策予算の程度の 4 つを使用する。これらの指標は以下の手順に従って作成される。

まず、セキュリティ対策の優先順位は、1) 新規サービスの展開、2) 既存サービスの現状維持、3) セキュリティ対策と順位をつけている。つまり、順位があがるにしたがって優先順位が高くなるといったものとなっている。次に、情報セキュリティ教育実施の程度は、1) 教育していない、2) 自主的に教育させている、3) SE（System Engeneer, システムエンジニア）を対象に教育している、4) 全社的に教育していると順位をつけている。これらの指標は、ISP の情報セキュリティ対策への態度（積極度）を表しているととらえることができる。つまり、順位があがるにしたがって情報セキュリティ教育の対象が大きくなるといったものになっている。

前者は経営戦略に関連するもので、後者は社内組織に関連するものである。

続いて、情報セキュリティシステムの導入数（種類）は種類数によって順位をつけ、そして情報セキュリティ対策予算の程度は、1) 予算なし、2) その他の経費として計上、3) 情報システム予算として計上、4) 情報セキュリティ予算として計上と順位をつけている。前者に関しては順位があがるにしたがってシステム導入数がふえるといったものとなり、また後者に関しては順位があがるにしたがって情報セキュリティ対策の予算が明確に決められるといったものとなっている。

これらの指標は、ISP の情報セキュリティ対策のための資金面に着目したものとなっている。

なお、図 3 にこれらの指標に関するアンケート調査の集計結果を示している。

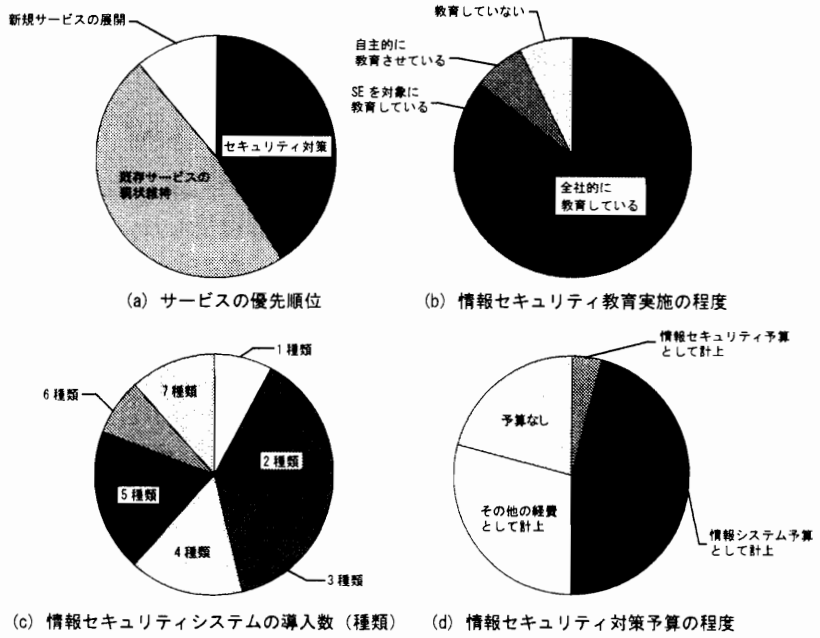


図 3: 情報セキュリティ対策の指標

経営パフォーマンスの指標として、売上高、総資産、従業員数（パート・アルバイトを含む従業員数）、個人からの契約収入を使用する。これらの基本統計量は 1 の通りである。平均値と中央値

の差異および標準偏差を見てわかるように、ISP 間に大きな違いがある[22]。

表 1: 経営パフォーマンス指標に関する基本統計量

	平均値	中央値	標準偏差	最大値	最小値
売上高（万円）	416,395.2	40,000	896,215.2	3,073,700	970
総資産（万円）	346,603.7	52,300	608,638.5	1,541,212	440
従業員数（人）	461.6	29	1623.1	7,700	1
契約収入（万円）	28,750	6,000	52,886.91	135,000	20

4.3 分析結果

分析には SPSS for Windows 13.01J（SPSS Inc.）を使用した。表 2 には、式 (1) によって計算したスピアマンの順位相関係数とこれらの相関係数を検定した結果がまとめられている。

表 2: スピアマンの順位相関係数と検定結果

	売上高	総資産	総従業員数	契約収入
サービスの優先順位	−0.138	0.016	−0.266	0.113
教育実施の程度	0.672**	0.764*	0.422*	0.677*
システム導入数（種類）	0.577*	0.462	0.485*	0.449
対策予算の程度	0.242	0.182	0.060	0.283

$^{*}: p < 0.05, ^{**}: p < 0.01$

分析の結果、情報セキュリティ教育実施の程度と経営パフォーマンスの指標（売上高、総資産、総従業員数、個人からの契約収入）においていずれも有意水準 1%もしくは 5%で正の相関関係があり、また情報セキュリティシステムの導入数（種類）と売上高および総従業員数においても有意水準 5%で正の相関関係があることが確認された[23]。つまり、情報セキュリティ教育を実施したりすることや、より多くの情報セキュリティシステムを導入したりすることと売上高を伸ばしたりすることに正の関係があることがわかった。この結果は、2 つの解釈が可能である[24]。

1 つ目の解釈としては、経営パフォーマンスを向上することで情報セキュリティ対策を積極に実施させると考えるものである。これは、経営状態がよくなるとセキュリティ教育を積極的に実施したり、より多くの情報セキュリティシステムを導入したりできるようになり、情報セキュリティのレベルを向上させることができるというものである。この時、横見・榎原・中庭・竹村 (2004) や

[22] これは、大手の全国系 ISP も数社含まれているためである。
[23] なお、これ以外のものについては、統計的に有意な結果が得られなかった。
[24] これらの因果関係については、この分析だけでは明らかにならないので、今後の研究の課題の 1 つにしたい。

横見 (2006) で主張されているように、経営パフォーマンスを向上させるため、まずISPは経営改善をおこなう必要がある。

2つ目の解釈としては、情報セキュリティ対策を積極的に実施することで経営パフォーマンスを向上させられると考えるものである。1節でも触れたように、情報セキュリティ被害が多い近年、個人や企業はよりセキュアなネットワーク環境を提供したり、情報セキュリティ被害に遭遇した時に対応が早く十分にできたりするようなISPを選択する可能性が高い。このことは個人や法人契約数や広告収入を増加させて、最終的に売上高を伸ばすことになるというものである[25]。特に、分析結果の安定性とISPの直面している経営状態を考えると、情報セキュリティ対策の中でも情報セキュリティ対策の強化が経営パフォーマンス向上に有効であるといえる。

特に、情報セキュリティ対策実施の程度と総従業員数、システム導入数と総従業員数の間に正の相関があることは興味深い結果である。これは、従業員数でISPの規模を測った場合、リーディング企業である大手の全国系ISPの方が地方都市の地域系ISPよりも情報セキュリティ対策に積極的に力を入れていることを意味している。このことからも、情報セキュリティ対策は重要な経営戦略の1つになっていることがわかる。

この分析結果を踏まえて、次節でISPのとるべき経営戦略と政府の役割について検討する。

5 結論と今後の展望

ISPに対するアンケート調査から、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明らかになった。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。この現状を改善するために、ISPのみならず、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。

情報セキュリティ対策と経営パフォーマンスに関する分析結果より、情報セキュリティ教育を実施したりすることや、より多くの情報セキュリティシステムを導入したりすることと売上高を伸ばしたりすることに正の関係があることがわかった。そのため、情報セキュリティ対策を十分施すには、まずISPの経営改善をおこなう必要がある。たとえば、提供しているアプリケーションサービスの中でもユーザのニーズの高いものに限定して投資をおこなうなど、経営戦略の見直しもその1つであると考える。また、経営の悪化の一因として、社団法人日本インターネットプロバイダー協会 (2003) や横見・榎原・中庭・竹村 (2004) で指摘されているようにバックボーンコストの存在が考えられる。各ISPの経営改善をおこなうためには、バックボーンネットワーク開放も解決策の1つであるが、保守管理や運用のあり方など多くの問題を含んでいる。そのために、本稿では、バックボーンネットワークの全面的な開放よりもその利用料（接続料）を適正かつ公正な水準にして、上位回線をもつISP（1次プロバイダ）は保守管理および設備投資をすべきであると提案する[26]。また、近年バックボーンネットワークについて地方自治体との連携（官民協業）の動きも見られの

[25] 総務省 (2005) によると、企業のインターネット広告費は2004年時点で1,814億円となり、5年間で7.5倍にまで急成長している。インターネット広告は、テレビ、新聞、雑誌に次ぐ広告メディアとなっている。

[26] ISPは1次プロバイダと2次プロバイダに大別できる。多くのISPは2次プロバイダである。なお、これらの特性などについては竹村 (2006a) を参照されたい。

で、それを利用することもISPの経営改善に役立つと考える。たとえば、秋田地域IX、兵庫情報ハイウェイや福岡ギガビットハイウェイなどは、いくつかの条件はあるものの無料もしくは安価で高速・大容量のネットワークを地元の企業に開放している。このように安価で高速・大容量ネットワークを提供することはISPに対する有効な支援策である。なお、この種のネットワークを利用するISPおよび企業に対して、一定の情報セキュリティレベルが確保されていなければ利用できないようにするなどの明確な規定（罰則を含む）が必要であると考える。

現在、ISP事業に対する国や地方自治体からの体系的な補助金制度は特にない[27]。アンケート調査において情報セキュリティ対策に特化した補助金制度の確立を求める意見もあった。しかしながら、本稿では補助金制度よりも、IT税制のように情報セキュリティシステムを導入したときに税制上の優遇措置がとられるような政策を国や地方自治体がおこなうことを提案する。

電気通信事業法改正（2004年4月1日施行）により、ISPの参入・退出規制は許可制から登録制および届出制に移行した[28]。それゆえに、ほぼ自由に参入・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、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[29]。

いずれの提案に対しても、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。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。なお、その活動はホームページにて報告されている[30]。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。

最後に、本稿の今後の課題と展望について述べる。本稿では簡単な定性分析を試みた。しかしながら、サンプル数が十分確保できなかったことや、ICT資産などに関する財務データが得られなかったため、ROSI[31]（Return on Security Investment）などの情報セキュリティ投資の定量的な

---

27) ただし、運営資金にベンチャー支援の補助金を活用したり、地方自治体がICT振興のために特別に設けた補助金を主要な設立資金源としたりするISPも一部存在している。

28) 電気通信回線設備の規模およびそれを設置する区域の範囲が総務省令で定める基準を超えていなければ、そのISPは届出通信事業者と呼ばれ、もし要件を超える設備などを有している場合は登録通信事業者と呼ばれる。

29) 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。

30) http://www.bits.go.jp/（2006年8月現在）

31) ROSIとは、情報セキュリティ対策コストに対する投資回収率のことを意味している。つまり、ROSIでは情報セキュ

経済効果を確認することができなかった。これは、今後の課題である。

参考文献

[1] 岡田昭宏・川原亮一 (2003),「IP 網におけるトラヒック特性分析の一考察」『信学技報』, NS2003-5, pp.17-20.

[2] 亀井聡・森達哉・大井恵太 (2003),「P2P ファイル共有の実態と課題」『信学技報』, CQ2003-40.

[3] 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/.

[4] 芝祐順・南風原朝和 (1990),『行動科学における統計解析法』東京大学出版会, pp.121-141.

[5] 情報セキュリティ検討会 (2006),『情報セキュリティ白書 2006 年度版』, pp.61-67.

[6] 重要インフラ専門委員会 (2005),『重要インフラの情報セキュリティ対策に係る基本的考え方』http://www.bits.go.jp/.

[7] 総務省 (2002),『情報通信白書』ぎょうせい.

[8] 総務省 (2005),『情報通信白書』ぎょうせい.

[9] 総務省 (2006),『情報通信白書』ぎょうせい.

[10] 竹村敏彦 (2006a),「インターネット・サービス・プロバイダの形態とサービス」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.19-32.

[11] 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.

[12] 内閣官房・総務省・経済産業省 (2005),『重要インフラにおける情報セキュリティに関するワークショップ』, pp.21-33.

[13] みずほコーポレート銀行産業調査部 (2002),「転換期を迎えたインターネットサービスプロバイダ業界－ブロードバンド時代におけるビジネスモデルの変化と業界再編の展望－」『みずほ産業調査』Vol.2 (2), pp.83-101.

リティ投資による生産性の向上や、リスク回避によるコスト削減について考える概念である。セキュリティの価値を明確な数字で表すには時間も労力も、膨大な実データの収集にかける必要があり、日本においてこれらの取り組みはまだ始まったばかりである。

[14] 峰滝和典 (2006), 「ISP（インターネット・サービス・プロバイダー）のネットワーク性と生産性」SJC Discussion Paper, DP-2006-006-J.

[15] 横見宗樹 (2006), 「全国系と地域系の効率性の差異に関するDEA分析」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.73-96.

[16] 横見宗樹・榎原博之・中庭明子・竹村敏彦 (2004), 「インターネット・サービス・プロバイダの技術効率性の計測－地域系ISPの現状と課題－」『公益事業研究』, Vol.56(3), pp.85-94.

[17] 横見宗樹・榎原博之・中庭明子・竹村敏彦・鵜飼康東（2004）, 「IT関連産業の技術的効率性の計測 – インターネット・サービス・プロバイダの現状と課題 –」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22号.