情報通信インフラにおける情報セキュリティ対策に関する研究（継続）

竹　村　敏　彦　　関西大学ソシオネットワーク戦略研究機構助教

1 はじめに

近年、多くの企業が直面している情報セキュリティに関する問題として、企業の情報セキュリティ水準が向上していないこと、情報セキュリティインシデント被害に遭遇することや労働損失が生じていることといった様々な問題が挙げられる。これらの問題に対する解決策として、暗号化技術等に代表される最新の技術に関する研究、経済学や経営学の視点からのマネジメントシステム等に関する定性的研究やゲーム理論を用いた理論的研究が盛んに行われている(1)。これらの研究蓄積は、規範としてすべき技術的対策やマネジメント的対策やその指針を教えてくれるが、それが実際うまく機能しているかまでは教えてくれない。また、田中・松浦［2003］や Chan and Ho［2006］等で指摘されているように、情報セキュリティの問題の多くは、技術の問題よりはむしろヒトや組織の問題に起因すると考えられる。その意味においても、経済学や経営学的視点（社会科学的視点）に立った定量的研究（実証研究）が必要とされる。しかしながら、国内外ともにその研究はまだ少ない(2)。本研究では、重要インフラの 1 つであるインターネットを提供しているインターネット・サービス・プロバイダ（ISP）に焦点を当て、情報セキュリティ対策の効果について分析を行う。ISP の情報セキュリティ対策は情報通信インフラを提供しているため、何らかの被害を受けた時の影響力を考えると、一般企業の対策よりも水準が高く設定される必要がある。勿論、本研究における分析は、一般企業に対しても応用することが可能である。例に漏れることなく、ISP および ISP の情報セキュリティ対策に関するデータの蓄積もほとんどされていない。それゆえに、ISP を対象としたアンケート調査を行うことにより、データの収集と蓄積を行うことができ、これらの問題を解決するために必要となる環境（制度・政策を含む）について更なる議論・分析を行うことができる。本研究では、これらのデータの収集と蓄積を行うとともに、それらを用いた定量的な分析を試み、情報インフラを担う ISP が安定したサービス提供を行うための具体的な政策の在り方について研究する。

以下、本稿は次の通り構成される。第 2 節においては、本調査研究の目的を明らかにし、情報セキュリティの経済分析の必要性と重要性について議論を行う。第 3 節においては、アンケート調査の概要を示すとともに、その結果から ISP の情報セキュリティ対策の実態を明らかにする。第 4 節では、アンケート調査結果等を用いて行った分析の一部を紹介する。そして、第 5 節にて本調査研究全体をまとめる。

2 本調査研究の目的

本調査研究の目的は 2 つある。1 つ目の目的としては、情報通信インフラとしてインターネットを個人や企業に提供している ISP を対象にアンケート調査を実施し、そこから情報セキュリティ対策の現状を把握することである。2 つ目の目的としては、情報セキュリティ対策および情報セキュリティインシデントを定性的かつ定量的に分析を行い、企業が取るべき対策と政府が取るべき政策について示唆を与えることである。

3 アンケート調査による ISP の情報セキュリティ対策の実態把握

3-1 ISP を対象とした情報セキュリティ対策に関するアンケート調査について

（1）アンケート調査の目的

インターネットは重要インフラの一つで、それを提供する ISP は社会的に重要な役割を担っている。しかしながら、ISP の情報セキュリティ対策および投資の実態に関する公表されたデータはなく、その現状把握は困難なものである。そこで、ISP に対して郵送アンケート調査を実施し、ISP の情報セキュリティ対策および投資の実態を把握し、またそこから ISP および企業、個人が実施すべき対策、また政府が実施すべき政策について明らかにすることが本研究調査の目的である。

（2）実施概況

「社団法人日本インターネットプロバイダー協会」のホームページに記載されていた 583 社の ISP を対象

に記名式の郵送アンケート調査を実施した[3]。なお、有効回答率は約 12%、アンケート実施期間は 2010 年 1 月から 2010 年 2 月である。

（３）質問項目

アンケート調査の質問項目は、大別して、1）事業状況、2）情報セキュリティ対策、3）情報セキュリティ被害・システムトラブルの遭遇状況、4）情報セキュリティに対する意識、5）政府の情報セキュリティ政策に対する意見、で構成されている。

3-2 ISP の情報セキュリティ対策の実態と現状

ここでは、アンケート調査結果の一部を紹介する。ISP の情報セキュリティに関する実態調査の詳細は竹村［2010］を参照されたい

（１）事業概況

年間売上高・純利益、加入者数、従業員数、提供している接続サービス・アプリケーションサービスや経営戦略等についての項目がある。

図 1 と図 2 には、ISP が提供している接続サービスとアプリケーションサービスの状況を表している。最も多くの ISP が提供している接続サービスは FTTH アクセスサービスであり、また、ほぼ全ての ISP が提供しているアプリケーションサービスとしてはメールやウェブサービスがあることがわかる。さらに、有料サービスとして IP 電話やホスティング･レンタルサーバを提供している ISP の割合も半数以上となっていることもわかる。

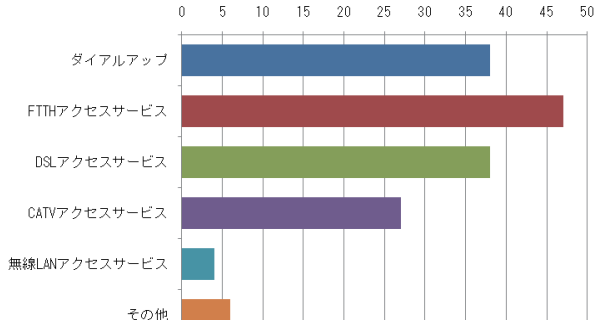


図 1　提供接続サービス

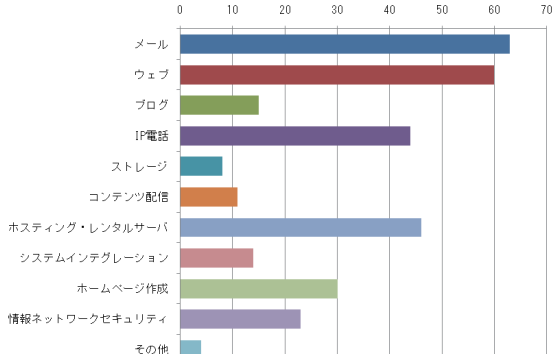
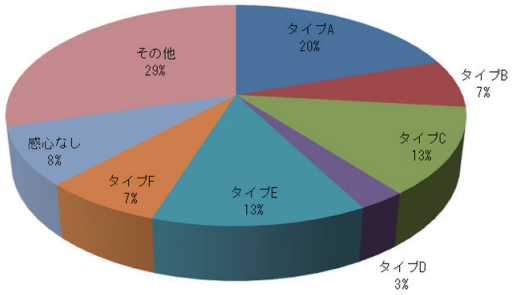


図 2　提供アプリケーションサービス

図 3 には、ISP が競争他社の経営戦略（価格、サービス内容、サービス品質）に対して関心があるものの順位を示したものである。タイプ A の割合が最も高くなっている。この他にも、従業員数に関しては正規社員とアルバイト・パートタイムともに必ずしも多いとは言えない状況にあることがわかっている。



タイプ
A：価格＞サービス内容＞サービス品質
B：価格＞サービス品質＞サービス内容
C：サービス内容＞価格＞サービス品質
D：サービス内容＞サービス品質＞価格
E：サービス品質＞価格＞サービス内容
F：サービス品質＞サービス内容＞価格

図 3　競争他社の経営戦略として関心

（２）情報セキュリティ対策

情報セキュリティに関する規定、管理担当者数、連絡体制、アップデート・パッチ適用状況、情報収集、ペネトレーション・システム監査・情報セキュリティ監査の実施状況、P2P の利用に関する自主規制状況、OP25B 導入状況、導入システム、情報セキュリティ教育の実施状況や今後の計画等についての項目がある。これらの中で、P2P の利用に関する自主規制状況、OP25B 導入状況と情報セキュリティ教育の実施状況につい

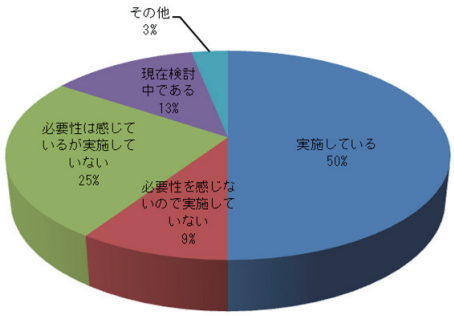


図 4　P2P 利用に関する自主規制状況

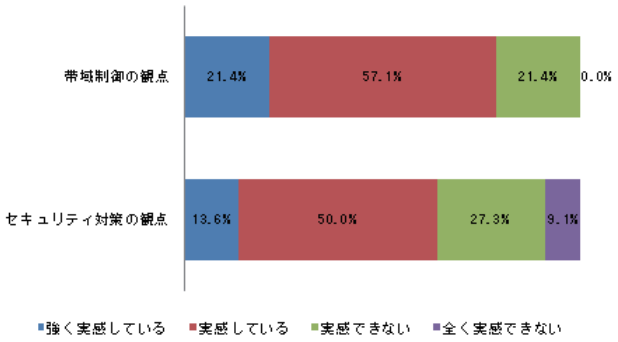


図 5　自主規制の効果の実感状況

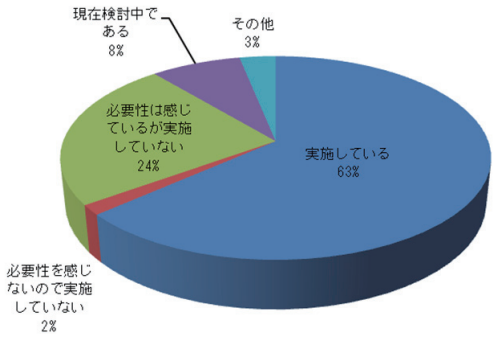


図 6　OP25B 導入状況

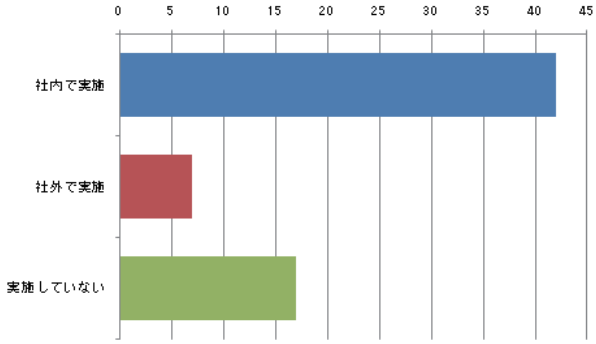


図 7　情報セキュリティ教育の実施状況

て図 4 と図 6 に示している。

P2P の利用に関する自主規制状況について見てみると、約半数の ISP が P2P の利用に関する自主規制を行っている。また、必要性を感じながらも実施していない ISP の割合が約 25%となっていることは注目すべきことである。実施に踏み切れていない理由としては、第 4 節で取り上げる通信の秘密に関する議論と密接に関連したものを挙げている。自主規制を行っている ISP の大半が図 5 にあるように、帯域制御（ネット混雑）およびセキュリティ対策の観点から効果を実感していると回答している。次に、OP25B の導入状況について見てみると、導入している割合は約 63%になり、昨年度と同様に、過去に行ったアンケート調査と比較して、その割合は高くなっている。また、OP25B を導入している ISP の約 56%が（迷惑メール被害の軽減の）効果を実感していると回答している。さらに、図 7 を見てわかるように、約 26%の ISP が情報セキュリティ教育の実施をしていないと回答しているが､その他の ISP は社内もしくは社外において実施していることがわかる。そして実施していない理由として多くの ISP が「人材不足」を挙げている。

（３）情報セキュリティ被害・システムトラブルの遭遇状況

不正アクセス被害、迷惑メール被害、マルウェアによる被害、システムトラブルの遭遇状況等についての項目がある。

図 8 を見てわかるように、不正アクセス被害、迷惑メール被害、マルウェアによる被害やシステムトラブ

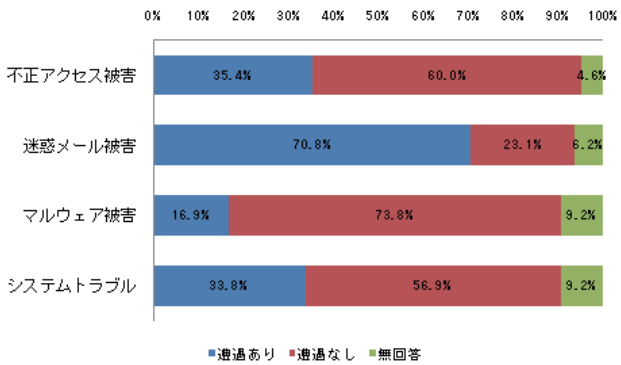


図 8　情報セキュリティ被害・システムトラブルの遭遇状況

ルに遭遇した ISP の割合は、順に約 35%、71%、17%、34%となっている。今回の調査では、これらの被害やトラブルに遭遇していても、ネットワークへの影響はそれほど出ていないという回答が多かった。特徴的なこととして、昨年度と比較しても迷惑メール被害の割合が急増している。この割合を軽減するためにも、全ての ISP での OP25B 導入が今後、期待される。

（４）情報セキュリティに対する意識

情報セキュリティ対策への優先度、効果的に思う情報セキュリティ対策、情報セキュリティ対策へのイメージ、関心のある最近の ICT 等についての項目がある。

図 9 には情報セキュリティに対する意識についてまとめている。一般的に、情報セキュリティ対策が企業の事業展開を困難にさせているという指摘もあるが、図 9 からは必ずしもその指摘は正しくないことがわかる。また、情報セキュリティ対策が企業価値を高めることを指摘している竹村・峰滝［2010］の主張をある意味、この結果は支持するものとなっている(4)。

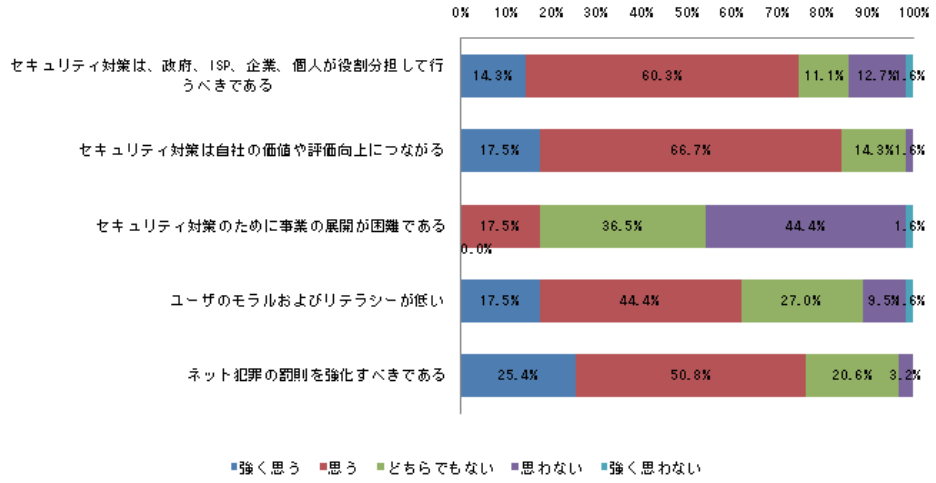


図 9　情報セキュリティに対する意識

（５）政府の情報セキュリティ政策に対する意見・要望

金銭的・非金銭的な公的補助の必要性や政策パッケージの必要性、セキュリティ政策の有効性の是非、認証制度への関心、政府への要望等についての項目がある。

図 10 を見てわかるように、金銭的な公的補助の必要性を求めている ISP の割合は約 54%であり、「どちらでも」という回答を含めるとその割合は約 89%になっている。また、非金銭的な公的補助（啓蒙活動や情報提供等）の必要性を求めている ISP の割合は約 57%であり、「どちらでも」という回答を含めるとその割合は約 90%になっている。政策や法律の有効性を感じている ISP の割合は約 39%と必ずしも高いものと言えない。図 11 には、政府や自治体への要望をまとめている。これを見てわかるように、ネット犯罪の罰則強化、国民、企業に対するリテラシーの喚起、無料の情報セキュリティ教育制度の充実を求める ISP が多いことがわかる。また、今回の調査では、特に「インターネットユーザのリテラシーの向上」を要望する ISP が多いことも確認されている。

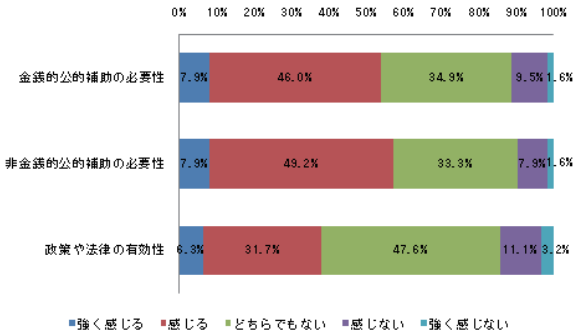


図 10　政策に対する意見

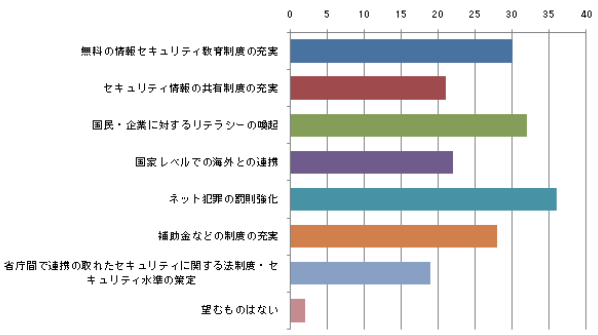


図 11　政府や自治体への要望

4 分析

4-1 ISP の情報セキュリティ対策と情報セキュリティインシデント遭遇確率に関する実証分析

ここでは、具体的に情報セキュリティインシデント被害に遭遇する確率を低下させる対策はどのようなものであるか、言い換えると、情報セキュリティインシデントに対してどのような対策が有効となるかについて実証分析を行う。なお、詳細については竹村・高田・小林・峰滝 [2010]を参照されたい。

本研究では、Takemura, Osajima and Kawano [2009]と同様に、情報セキュリティ対策と情報セキュリティインシデント被害との関係を調べるために、式 (1)のロジスティック回帰モデルを採用する。

$$\log (p_j/1-p_j)=a+b_m X_m + cZ_C \qquad (1)$$

ここで、p_jは ISP が情報セキュリティインシデント j に遭遇する確率を表す。なお、本研究では、情報セキュリティインシデント j としては、不正アクセス、マルウェア、迷惑メールとシステムトラブルの 4 つを考える。また、対策に関連する説明変数 (X_m) としては、教育 (XE)、ユーザに対する注意喚起 (RU)、システム導入 (SI)、情報セキュリティ監査 (ISA)、また、ISP 特性 (Z_c) として、サービス提供エリア (AREA) を用いる。

式 (1)の右辺の係数パラメータは対数オッズ比を表しており、これは、リスク指標の一つとして解釈することができる。例えば、説明変数 X_m'の係数パラメータが正 (b_m'>0) であれば、それが変化したとき、情報セキュリティインシデントに遭遇する確率は EXP[b_m']倍高くなることを意味する。逆に、その値が負であれば、遭遇確率は低くなる。それゆえに、対策が有効であれば、被害遭遇確率は下がるため、両者には負の関係 (b_m'<0) があることが期待される。

次に、ISP の特性としてサービス提供エリアを考える。榎原・中庭・竹村・横見 [2006]でも指摘しているように、地域系 ISP と全国系 ISP の経営状態には大きな違いがある。そこで、われわれは地域系 ISP と全国系 ISP という特性と被害遭遇確率に関係があると考え、これを 1 つの変数として用いる。

ロジスティック回帰式による分析結果を通じて、情報セキュリティインシデント被害に遭遇する確率を低下させる対策はどのようなものであるか、言い換えると、情報セキュリティインシデントに対してどのような対策が有効となるかについて議論の材料を提示することができる。

式(1)の係数パラメータを変数減少法に基づく最尤法によって推計した結果を示す。表 1 と表 2 は、検定に用いられる統計量と式 (1)の推計された係数パラメータをまとめたものである。なお、定数項についてはここでは省略している。

表 1　統計量のまとめ

	1) 不正アクセス被害	2) マルウェアによる被害	3) 迷惑メールによる被害	4) システムトラブル
-2 対数尤度	64.575	9.207	45.283	58.936
Cox-Snell R^2	0.085	0.695	0.331	0.046
Nagelkerke R^2	0.113	0.926	0.441	0.061
正誤率	65.3	97.8	76.1	56.8

表 1 を見てわかるように、Cox-Snell R^2 と Nagelkerke R^2 は 1) 不正アクセス被害と 4) システムトラブルにおいて必ずしも高くない。しかしながら、正答率は 4) システムトラブルのケースで一番低く 56.8%であるが、全体的に見ていずれの結果もそれほど正答率が悪いとはいえない。

表 2　推計結果

	係数 (B)		S.E.	EXP[B]
1) 不正アクセス被害	b_{RU}	-0.446	0.221	0.640184
2) マルウェアによる被害	b_{RU}	-5.682	2.076	0.003407
	b_{SI}	0.465	0.270	1.592014
3) 迷惑メールによる被害	b_{RU}	-1.831	0.654	0.160253
	b_{SI}	0.256	0.161	1.291753
	b_{ISA}	2.070	0.866	7.924823
4) システムトラブル	b_{RU}	-0.321	0.228	0.725423

表 2 から、変数の多くが変数減少法により、式 (1)の変数の候補から取り除かれていることがわかる。4 つの情報セキュリティインシデントに共通して統計的に有意となっている変数は、「ユーザに対する注意喚起」であり、その係数パラメータはいずれも（大きさは異なるものの）負の値をとっている。これは、ユーザに対してセキュリティに関する注意喚起を行うことで、その ISP が情報セキュリティインシデントの被害に遭遇する確率を低くすることができることを意味している。そして、この分析の結果から、ユーザに対してセキュリティに関する注意喚起を行うことが情報セキュリティ対策として有効となるといえる。

一方で、2) マルウェアによる被害と 3) 迷惑メールによる被害に関しては、導入システムの種類（数）の係数パラメータは統計的に有意となり、その値は正の値をとっている。これは、情報セキュリティを確保するために導入しているシステムの種類（数）が多くなるにつれて、マルウェアや迷惑メールによる被害に遭遇する確率が高くなる（遭遇しやすくなる）ことを意味している。これは、Takemura, Osajima and Kawano [2009]においても同様のことが確認され、彼らは、ISP の人材不足の問題から、この結果について、多くの ISP は人材不足の問題に直面している状況においてセキュリティ以外にもあるサーバやシステムを運用管理することには限界があり、逆に能力を超えた運用管理を強いることによって、見過ごしやその他のヒューマンエラーが出やすくなり、それが被害遭遇確率を高めているのではないかという解釈を与えている。別途実施したヒアリング調査等からもこの解釈はある程度の妥当性をもっていることがわかっている。

4-2 インターネットユーザの情報セキュリティ意識に関する定量分析

ISP に対する郵送アンケート調査から、インターネットユーザの情報セキュリティおよびその対策に対する意識が ISP の対策として重要なキーになることが確認されたものの、インターネットユーザの情報セキュリティおよびその対策に対する意識に関する経済・経営学的視点からの定量分析は、これまでほとんど行われてこなかった。そのため、本研究では、インターネットユーザの情報セキュリティ意識に関する定量分析を試みた。なお、詳細については竹村・海野[2009]や Takemura and Umino [2009]を参照されたい。

分析には、インターネット（Web）アンケート調査法により収集・蓄積した「インターネットおよび情報セキュリティ意識に関する調査」の個票（ミクロ）データを用いる(5)。これらは、インターネットユーザを対象に調査されたものであり、インターネット未利用者は一切含まれていない。サンプルの事前割付は、年齢、居住地域及び性別の 3 軸で行っている(6)。なお、サンプルサイズは 1483 件である。

情報セキュリティ意識に関する指標として表 3 にある指標を用いている。いずれの指標も 5 段階（1～5）で質問しており、意識が低いと小さい値、逆に意識が高いと大きな値をとるように調整を行っている。

表 3　情報セキュリティ意識に関する指標

変数	質問内容	平均	標準偏差
X_1	コンピュータウィルス対策ソフトを入れていないコンピュータを使うことについてあなたは問題があると思いますか	4.00	0.905
X_2	チェーンメールを受け取ったとき、それを友人や知人などに送ることにあなたは問題があると思いますか	4.15	0.894
X_3	セキュリティ対策をして安心感は高まりましたか	2.57	0.754
X_4	セキュリティ対策は ISP の問題であり、個別に対策すべき事項ではない	3.48	0.832
X_5	現在と 1 年前と比べて、あなたご自身の情報セキュリティへの態度（情報管理などの考え方）は変化しましたか	3.51	0.648
X_6	個人のセキュリティ対策は必要と思いますか	4.04	0.828

表 4　カテゴリー（個人属性）に関する情報

内容	説明
性別	1　男性　2　女性
年齢層	1　20代　2　30代　3　40代　4　50代　5　60代　6　70歳以上
情報セキュリティ教育	0　誰からも教わっていない　1　研修や大学教育で教わった
インターネット歴	1　1 年未満　2　1～2 年（未満）　3　2～3 年　4　4～5 年 5　6～7 年　6　8～9 年　7　10 年以上

表 4 には、分析で用いるカテゴリー（個人属性）に関する情報を示している。その内容は、性別、年齢層、情報セキュリティ教育を受けているか否か、インターネット歴といったものである。

本研究では、表 4 にあるカテゴリーをもとに、それぞれの個人属性によって、情報セキュリティ意識が異なるか否かを、Mann-Whiteney 検定や Jonckheere-Terpstra 検定を通じて、様々な属性により異なるか否か

の検証を行う(7)。その分析結果が表 5 である。

これらの結果から、個人属性によってインターネットユーザの情報セキュリティ意識に差異がみられる。例えば、Mann-Whitney の U 検定を行った結果及びそれぞれの統計量から、情報セキュリティ教育を受けたユーザは、受けていない（独学も含む）ユーザよりも情報セキュリティ意識が高くなっていることが確認できる。この意味においても、情報セキュリティ教育の充実が重要であるといえる。また、Jonckheere-Terpstra 検定（J-T 検定）を行った結果及びそれぞれの統計量から、全体的に、年齢層が上がる（インターネット歴が長くなる）につれて、情報セキュリティ意識が高くなる傾向があることもあわせて確認できる。

表 5　分析結果

	性別			年齢層			
	Mann-Whitney の U	Z 値	有意確率	観測された J-T 統計量	J-T 統計量の標準偏差	標準化された J-T 統計量	有意確率
X_1	269065.0	-0.727	0.467	452564.5	8854.507	-0.554	0.579
X_2	271556.5	-0.412	0.681	424521.0	8751.454	-3.765	0.000***
X_3	259372.5	-2.030	0.042**	453068.0	8607.355	-0.512	0.609
X_4	257806.5	-2.210	0.027**	426447.0	8714.653	-3.560	0.000***
X_5	252905.5	-2.975	0.003***	462095.5	8348.201	0.554	0.580
X_6	269633.5	-0.677	0.499	441682.0	8562.301	-1.844	0.065*
	情報セキュリティ教育			インターネット歴			
	Mann-Whitney の U	Z 値	有意確率	観測された J-T 統計量	J-T 統計量の標準偏差	標準化された J-T 統計量	有意確率
X_1	136712.5	-2.004	0.045**	435992.5	8513.524	4.973	0.000***
X_2	135339.0	-2.271	0.023**	455819.0	8414.449	7.388	0.000***
X_3	140069.0	-1.457	0.145	382560.0	8275.909	-1.341	0.180
X_4	127571.0	-3.662	0.000***	444931.0	8379.063	6.119	0.000***
X_5	114585.0	-6.235	0.000***	419198.5	8026.757	3.182	0.001***
X_6	133736.0	-2.611	0.009***	442415.0	8232.584	5.923	0.000***

***: p<1%、**：p<5%、*：p<10%

4-3 プロバイダ責任法に対する法的解釈に関する研究

インターネット上における権利侵害があった場合に ISP が負う損害賠償責任の範囲や情報発信者の情報の開示を請求する権利等を定めた法律に「特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律」（以下「プロバイダ責任制限法」と呼ぶ）がある。そこで規律されている事業者の送信防止措置や発信者情報開示請求への応諾をめぐって、近年、憲法 21 条（通信の秘密、表現の自由）との関係でその合憲性について議論がある。本研究では、憲法上の通信の秘密の意義や通信の秘密と表現の自由との関係から、プロバイダ責任制限法の合憲性について、従来の憲法 21 条 2 項後段の解釈論を超えた新たな視点から論じている。なお、議論の詳細については海野・竹村［2010]を参照されたい。

このことは、近年米国を中心として展開されている「ネットワーク中立性」の議論と密接に関連しているものであり、上述のアンケート調査からも、P2P の自主的な利用規制や OP25B といった対策が総務省で違法ではないと一つの見解が出されているものの、実施に踏み切れていない ISP の数社は、ユーザの利便性を優先することとともに「通信の秘密がネックとなる」と回答している。これらは ISP に求められる有効な対策であるが、合法性が保証されたものではないといったことから、実施に踏み切れていないと言える。つまり、これらの問題を解決しなければ、ISP のみならず、ユーザである企業や個人にとっても経済的な不利益（情報セキュリティインシデント被害等）を被ることになる。

法学的なアプローチから、プロバイダ責任制限法の規律について以下のような考えに至った。プロバイダ責任制限法は憲法問題を提起する立法措置であり、その合憲性を判断するためには、基本権保護義務論の基本的考え方を手がかりとする新たな法解釈の枠組みが必要であることが明らかである。プロバイダ責任制限法は、立法権による基本権保護義務の履行の結果にほかならず、その規定に内在する表現の自由や通信の秘密不可侵に対する制約についても当該義務として行われる基本権法益の保護の要請から、内在的制約として

正当化されることとなる(8)。すなわち、立法権は、基本権保護義務の履行に当たり、これらの基本権法益を保護することを権利侵害情報に関する表現の自由や通信の秘密不可侵の保障よりも優先させる必要があったということである。したがって、プロバイダ責任制限法の規律は表現の自由や通信の秘密不可侵との相克を超えて合憲であるという 1 つの結論を与えることができる。

5 まとめ

本調査研究では、ISP の情報セキュリティ対策の現状の把握を行うとともに、情報セキュリティ対策および情報セキュリティインシデントを定量的に分析してきた。現状把握および 2 つの実証分析については、すでに上述した通りである。多くの ISP は厳しい経営状態にあるにも関わらず、ユーザに安心・安全なインターネットを提供することの必要性を鑑みて、努力を重ねている。一般企業は、情報セキュリティ対策とその意識について、必要とされる情報セキュリティ水準の違いはあるものの、ISP から学ぶべき点が多くあると思われる。本調査研究が学術的のみならず、現実世界の情報セキュリティ対策に寄与することを期待したい。

今後もこのような調査研究を継続し、この種の情報セキュリティ対策に関する研究の蓄積を行っていく。学術研究にとどまるのではなく、研究成果を様々な形で政策担当者や情報セキュリティ関連組織をはじめとして積極的に外部発信することによって、実際の政策決定の材料を提示していきたい。これは情報セキュリティというテーマを扱う上で重要なことであると考える。さらに、ISP だけでなく、情報通信業全体での情報セキュリティ対策の実態調査を行い、日本の情報通信インフラにおける情報セキュリティ対策の実態把握を試みたい。その意味において、本研究はその第一歩である。

【参考文献】

Anderson, R. and Moore, T., Information Security: Where Computer Science, Economics and Psychology Meet. Philosophical Transactions of the Royal Society, Vol.367, pp2717-2727, 2009

Camp, L.J., The State of Economics of Information Security. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.99.6038&rep=rep1&type=pdf, 2006

Chan, S.E. and Ho, C.B., “Organizational Factors to the Effectiveness of Implementing Information Security Management” Industrial Management & Data Systems, Vol.106, No.3, pp345-361, 2006

Takemura, T., Osajima, M., Kawano, M.: “Economic Analysis on Information Security Incidents and the Countermeasures: The Case of Japanese Internet Service Providers” K. Jayanthakumaran (Ed.), Advanced Technologies, INTEH, Chapter 5, pp73-89, 2009

Takemura, T., Umino, A.: “A Quantitative Study on Japanese Internet Users’ Awareness of Information Security: Necessity and Importance of Education and Policy” The Proceedings of World Academic of Science, Engineering and Technology, Vol.60, pp638-644, 2009

海野敦史・竹村敏彦:「プロバイダ責任制限法の規律と通信の秘密の保障との相克」『公益事業学会第 60 回大会研究報告予稿集』pp83-88, 2010

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, 2006

竹村敏彦:「第 4 回インターネット・サービス・プロバイダの情報セキュリティに関する実態調査報告書」関西大学, 2010

竹村敏彦・海野敦史:「インターネット利用者の情報セキュリティ意識に関する研究」『情報通信ジャーナル』H21 年 8 月号, pp13-22, 2009

竹村敏彦・高田義久・小林徹・峰滝和典「日本の ISP の情報セキュリティ対策に関する実証分析」『日本経済政策学会第 67 回全国大会報告要旨集』pp41-42, 2010

竹村敏彦・峰滝和典:「情報セキュリティマネジメントとその効果に関する実証分析－教育・情報共有をサポートする政策の必要性」『経済政策ジャーナル』第 7 巻第 2 号, pp46-49, 2010

田中秀幸・松浦幹太:「情報セキュリティ・マネジメントの制度設計」日本セキュリティ・マネジメント学会・特定非営利活動法人ネットワークセキュリティ協会主催、Network Security Forum 2003, pp1-17, 2003

(1) これまでの情報セキュリティの経済学（Economics of Information Security）に関する包括的なサーベイは Camp [2006]や Anderson and Moore [2009]等を参照されたい。情報セキュリティの経済学における実証分析は、学術的な意義だけでなく、実務的にも大きな意義を持っており、情報セキュリテ

ィに関する政策の一材料となりうる。そのため、今後更なる研究を行い、その蓄積を進められていく必要がある。

(2) その理由として、経済学者や経営学者の多くが ICT のもたらす正の経済効果を測定することにのみ関心がいっていたため、情報セキュリティに関する問題がそれほど大きなものであると思っていなかったことや、そもそも分析に利用できるミクロデータがなかったもしくは容易に利用できなかったことが挙げられる。

(3) 平成 22 年 6 月現在、社団法人日本インターネットプロバイダー協会 (http://www.jaipa.or.jp/) の Web サイトに記載された ISP の数とは異なっている。

(4) 竹村・峰滝 [2010]は、企業の情報セキュリティ担当者を対象とした Web アンケート調査によって収集したミクロデータを用いて、情報セキュリティ対策、特にマネジメント対策と企業価値に結びつく対策の効果の関係を定量的に分析し、いくつかの対策が企業価値向上につながることを明らかにしている。詳細については、竹村・峰滝 [2010]を参照されたい。

(5) 関西大学ソシオネットワーク戦略研究センターが 2009 年 3 月に Web アンケート調査形式で実施した「インターネットおよび情報セキュリティ意識に関する調査」によって収集されたミクロデータを用いる。

(6) このアンケート調査の事前割付には、「住民基本台帳に基づく人口・人口動態及び世帯数 (平成 20 年 3 月 31 日現在)」の参考資料 3 (都道府県別の年齢階級別人口) を用いて、年齢 (20 歳以上)、居住地域および性別を用いている (http://www.soumu.go.jp/menu_news/s-news/2008/ 080731_6.html)。

(7) Mann-Whitney の順位和検定(Mann-Whitney の U 検定)は 2 群間の中央値の差異を調べる検定であり、得られたデータそのものではなく、小さい順に並べたデータの順位和を検定統計量 (U) とする。ただし、データに同一順位がある場合には、平均順位を用いて計算する。これらの統計量から、標準偏差と平均値を用いて Z 値を計算する。U の分布は近似的に正規分布にしたがうとされるため、標準正規分布表から漸近有意確率を求める。なお、両者の検定における帰無仮説は、「2 つのカテゴリーの中央値に差異はない」である。

3 群以上の中央値の差異を調べる検定として Jonckheere-Terpstra 検定がある。この検定は、Mann-Whitney の順位和検定と同様に、データの順位を利用して検定統計量を計算する。Jonckheere-Terpstra 検定では、J-T 統計量から、標準偏差と平均値を用いて標準化された J-T 統計量を計算する。そして、その統計量の分布は近似的に正規分布に従うとされるため、標準正規分布表から漸近有意確率を求める。なお、両者の検定における帰無仮説は「それぞれ (3 つ以上) のカテゴリーの中央値に差異はない」である。

(8) ここで保護される基本権法益には、名誉やプライバシー等に関する人格権の他、通信の秘密不可侵に内在する規範的権利としとしての通信制度の安定的運営を求める権利、財産権、裁判を受ける権利に関する法益等が含まれる。

〈発　表　資　料〉

題　　名	掲載誌・学会名等	発表年月
An Economic Approach to Issues on the Information Security	RCSS Discussion Paper Series, No.86	2009 年 7 月
An Empirical Analysis on Information Security Countermeasures	The 2st International Conference on Social Sciences (Social Sciences Research Society)	2009 年 9 月
インターネット利用者の情報セキュリティ意識に関する研究	情報通信ジャーナル, H21年8月号	2009 年 8 月
A Quantitative Study on Information Security Awareness of Japanese Internet Users and Policy Study	the 7th International Conference on Socionetwork Strategies (Kansai University)	2009 年 10 月
インターネットユーザの情報セキュリティ意識に関する分散分析	早稲田大学大学院 国際情報通信研究科紀要 2008-2009	2009 年 10 月
Positive Analysis on Vulnerability, Information Security Incidents, and the Countermeasures of Japanese Internet Service Providers	International Journal of Business, Economics, Finance and Management Sciences, Vol.1, No.3	2009 年 7 月
A Quantitative Study on Japanese Internet Users' Awareness of Information Security: Necessity and Importance of Education and Policy	The Proceedings of World Academic of Science, Engineering and Technology, Vol.60	2009 年 12 月
An Economic Approach to Issues on the Information Security	International Workshop on Information Systems for Social Innovation 2009	2009 年 9 月
日本の ISP の情報セキュリティ対策に関する実証分析	第67回日本経済政策学会全国大会	2010 年 5 月
プロバイダ責任制限法の規律と通信の秘密の保障との相克	公益事業学会第 60 回大会	2010 年 6 月