ネット上における行動が与える社会・経済的インパクトに関する研究

代表研究者　　竹　村　敏　彦　　佐賀大学　経済学部　准教授
共同研究者　　三　好　祐　輔　　香川大学　大学院地域マネジメント研究科　准教授

1 はじめに

インターネットは、グローバルなコミュニケーションツールとしての個人の生活の質の向上に大きく寄与しているとともに、企業活動においてもまたビジネスプラットフォームとして重要な役割を果たしていることは疑いもない事実である。インターネットはこのようにわれわれにとって正の影響をもたらす有意義なツールであるだけはなく、負の影響ももたらすことが指摘されている。それが、コンピュータウイルスなどによるインターネットインシデント被害やリテラシーの低さ等に起因する「炎上」(flaming) がもたらす企業の信頼失墜などである。炎上とは，インターネット上のコミュニケーションに関するトラブルの１つで，ブログなどの個人向け CGM のコメント欄などに批判や誹謗中傷が殺到する現象のことである[1)]。

さらに、これらの情報セキュリティの不安やインターネット上での行動はプライバシーに対する意識と密接に関連しており、新たなビジネスを創出するであろうビッグデータを用いたビジネスやオンラインサービスの普及にも負の影響を与えていると思われる。

本調査研究では、まず社会心理学の調査研究および近年注目されている行動経済学の視点を踏まえて、アンケート調査を実施し、インターネット上での行動やセキュリティ意識、プライバシー意識を把握することにある。次に、アンケート調査の結果を定量的に分析し、「炎上」に参加している個人のネット行動および意識についてメカニズムを調べる。そして、この分析結果を踏まえて、企業が取るべき具体的な対策や政府が示すべき指針を提示する。

2 本調査研究の背景

社会心理学の分野で、インターネットにおける行動・心理について研究されており、CMC (Computer Mediated Communication) は対面コミュニケーション (Face to Face Communication) よりも攻撃性や自己開示を促進する可能性があることが指摘され、またネット炎上やサイバーカスケード（インターネット上における集団極性化）についての心理学的見地からの分析も進められている (Joinson; 2003、辻; 2008、三浦他; 2009、田代; 2012)。ネット炎上によって個人だけでなく、ソーシャルメディアリスクという言葉があるように、その個人の属している組織にもダメージを与えることがわかっている。また、炎上させた個人だけでなく、その炎上に加担した個人に対しても法的責任が追及されることも指摘されている (永井; 2014)。このことを鑑みると、インターネット上の行動、とりわけ炎上の問題を経済学のフレームワークにおいても分析を行う必要があるが、企業や国全体の被害損失額試算モデルや経済行動モデルといったものはまだ示されていない状況にある。その理由として、社会心理学の調査研究がすぐに経済行動モデルには援用されにくかったことやネット炎上といった現象自体が企業経営に与えるインパクトはそれほど大きくないと考えられていたことなどが挙げられる。経済学や経営学ではインターネットの正の影響にのみ注目が集まり、負の影響についての検証がほとんど行われてこなかった。これらの負の影響に注目した研究分野は「セキュリティエコノミックス」(Economics of Information Security) と呼ばれているが、まだ日本ではそれほど浸透しているとは言いがたい。

3 SNS ユーザの意識・行動等に関する調査

3-1 アンケート調査概要

（１）調査目的

われわれは、SNS ユーザの情報セキュリティ・プライバシーに対する意識やインターネット上での行動 (以下、ネット行動)、とりわけ昨今問題となっているインターネット上での避難・批判・誹謗中傷など等のコメントが殺到する状態、いわゆる「炎上」に参加しようとしている個人のネット行動、についての実態を把握

することを目的として、2015 年 3 月に「SNS ユーザの意識・行動等に関する調査 2015」（以下，「本調査」と称す）と題したインターネットアンケート調査を実施した。

（２）調査形式

本調査はインターネット調査形式にて実施されたものである [2)]。この調査形式を採用した理由として、調査環境の劇的な変化（回収率の低下，プライバシーや個人情報保護法への過剰反応による拒否率の上昇など）に加えて、Kotulic and Clark（2004）などで指摘されているように、情報セキュリティ特有の問題点として多くの企業が部外者にセンシティブな情報を出したくないといった理由により調査協力がそもそも得られない点をカバーし、効率よく調査対象者を抽出するためである。インターネット調査の利用に関しては是非があるが、この調査手法の利用可能性・妥当性については労働政策研究・研修機構（2005）、星野（2009）、石田他（2009）などを参照されたい.

（３）調査対象

調査対象者は SNS を利用している個人を対象としているため、まず調査対象者であるかを調べるための事前調査を約 2 万人に対して実施し、その中から条件を満たす 1,260 人を抽出し、本調査に回答してもらうという 2 段階の方式を採用している．また，表 1 のように事前に割付を行い、オーバーサンプリングや，計測している回答時間から一般的な回答者と比べて回答時間が早い者を不良回答者として取り扱いサンプルから外すなどして、最終的に 1,238 人の有効回答数を得ている。

表 1　調査対象者の割付

属性 1	属性 2	人数（割付）
社会人	20 代	155
	30 代	155
	40 代	155
	50 歳以上	155
その他	学生	309
	主婦・主夫・無職	309

（４）質問項目

本調査の質問項目は、SNS の利用状況、情報セキュリティ意識、プライバシー意識、情報セキュリティ行動、情報リテラシー、リスク許容度など多岐にわたり、質問総数は約 60 問である [3)]．質問項目は、Takemura（2011）、竹村・花村（2014）や情報処理推進機構（2015）などで用いられているものを参考に作成している。

3-2 SNS ユーザの実態と現状

本調査の質問項目数は約 60 問であるために、ここではその調査結果の一部を紹介する。

（１）インシデント等に関する主観的リスク評価・抵抗感

図 1 にはコンピュータウイルスなどをはじめとするインシデント等に関する主観的なリスク評価を質問した結果を示している。「情報漏洩」にリスクを感じている（「とてもリスクがある」「ある程度リスクがある」と回答している）割合が 70.3%と最も高いが、自身のブログ等の炎上にリスクを感じている割合は 37.8%にとどまっている。図 2 には他人のブログを炎上させること等についての抵抗感を示している。図 2 を見て分かる

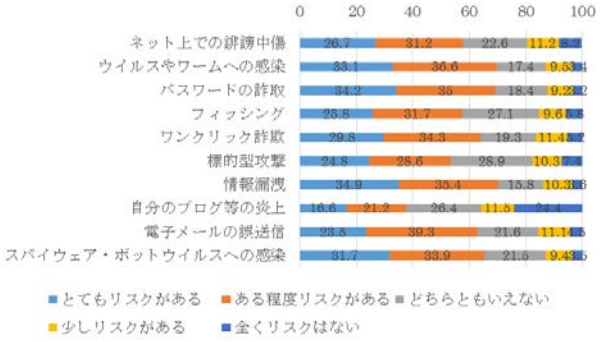


図 1：インシデント等に関する主観的リスク評価

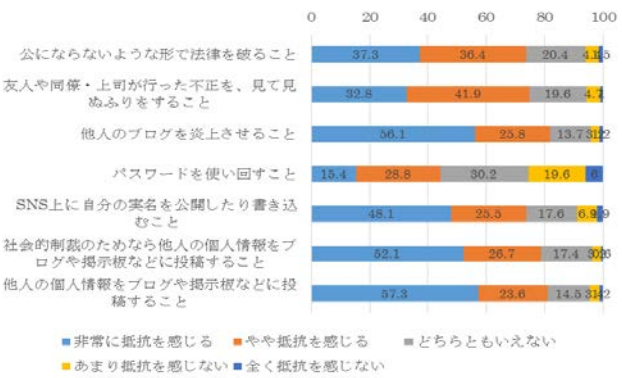


図 2：抵抗感

ように「他人の個人情報をブログや掲示板などに投稿すること」に非常に抵抗を感じる割合は 57.3%であるのに対して、同じ投稿することでも「社会的制裁のため」という表現が入ることで非常に抵抗を感じる割合は 5.2 ポイント低下している。また、「パスワードを使いまわすこと」については抵抗感を感じている（「非常に抵抗を感じる」「やや抵抗を感じる」と回答している）割合が約 45%にとどまっていることがわかる。

（２）利用アカウント数・パスワード管理

図 3 にはインターネットで利用している ID（アカウント）数について質問した結果を示したものである。図 3 を見てわかるように、3～5 種類と回答している割合が約 36%で最も多く、続いて 6～10 種類と回答している割合が約 23%となっている。また、11 種類以上と回答している割合は約 15%となっており、複数のアカウントを利用している個人が多いことがうかがえる。図 4 にはそのアカウントおよびそのパスワードの管理・設定について質問した結果を示している（この質問は複数選択することが可能である）。「パスワードは誕生日など推測されやすいものを避けて設定している」「パスワードはわかりにくい文字列（8 文字以上、記号を含む）を設定している」と回答している者の数が多いものの、「基本的に変更しない（システムから強制されたら変更）」や「1 種類のみを共通で使っている」（パスワードの使い回し）と回答している者の数もそれほど少なくないことも図 4 からわかる。

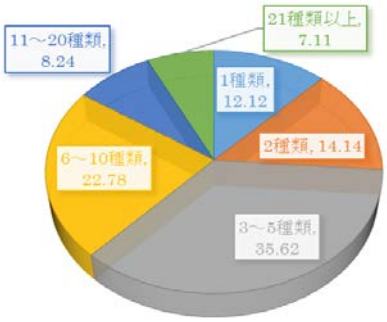


図 3：利用アカウント数

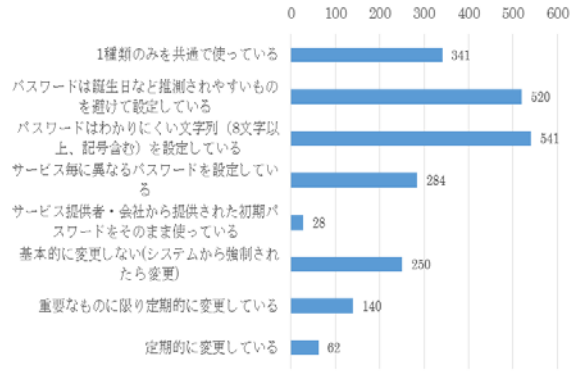


図 4：パスワードの設定方法

（３）悪意ある投稿

情報処理推進機構（2015)にもある悪意ある投稿経験について質問した結果を図 5 に示している [4)]。回答者の約 93%は悪意ある投稿をした経験がないと回答しているものの、約 7%の回答者が何らかの悪意ある投稿をした経験を有していることがわかった。この割合は情報処理推進機構（2015)の結果よりも少ないものの、複数のサービスで悪意ある投稿をしている回答者も少なからずいることがうかがえた。また、「下品な言葉を含む内容」（85 人）と「他人の発言を非難する内容」（84 人）となり、他の内容よりもわずかながら多いことが

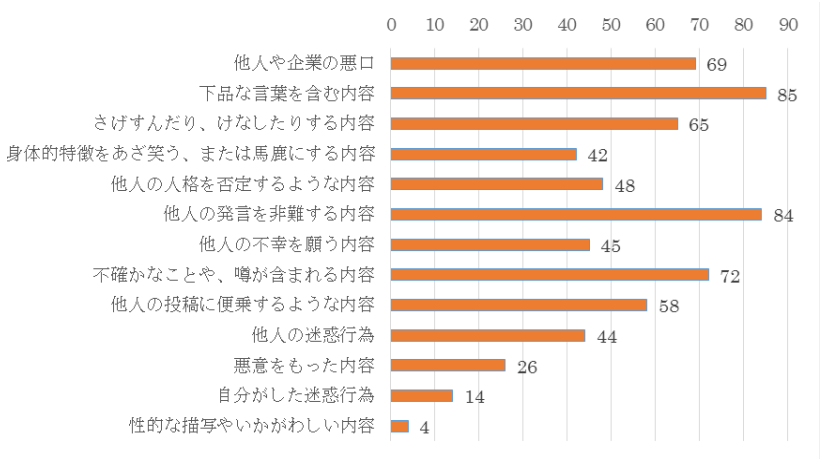
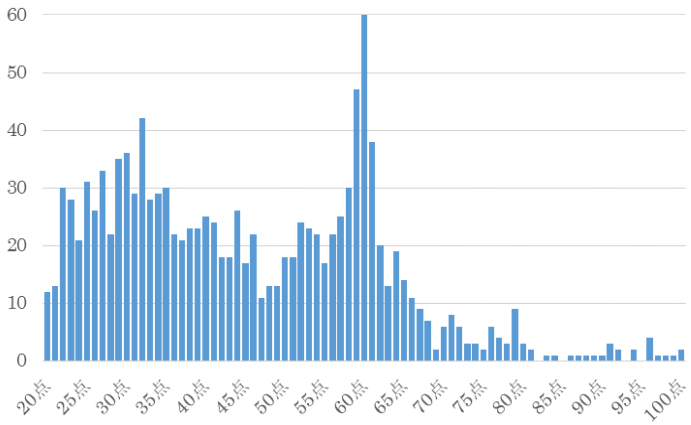


図 5：悪意ある投稿

わかる。さらに、これらの悪意ある投稿をする理由については情報処理推進機構（2015）と同様に「人の意見に反論したかったから」「人の投稿やコメントを見て不快になったから」と回答している者が多かった。

（４）インターネット依存度

インターネットの普及とともに、インターネットに依存するユーザの実態が明らかになり、これもまた様々な問題が指摘されている。ヤング（1998）では 20 項目からなる診断基準であるインターネット依存度テスト（IAT; Internet Addiction Test）が提唱され、幅広く使われている [5]。インターネット依存度テストの結果の分布を図 6 に示している。平均的なユーザは回答者の約 43%となり、それ以外についてはインターネット依存度が少し疑われることがわかる（70～100 点となっている回答者の割合は約 5%程度であった）。



【依存度判定基準】

・20～39 点：平均的なオンライン・ユーザーです。
・40～69 点：インターネットによる問題があります。インターネットがあなたの生活に与えている影響について、よく考えてみてください。
・70～100 点：インターネットがあなたの生活に重大な問題をもたらしています。

図 6：インターネット依存度

（５）利用可能性ヒューリスティック

利用可能性ヒューリスティックとは、簡単に言うと、想起しやすい物事の確率を高く見積もる傾向のことを意味する。これはあらゆる物事とその確率を正しく認識していないことから生じる認知的バイアスである。また、インターネットでは様々な情報があり、その真偽を確認することをせずに行動を起こすことも少なくない。そこで、本調査では簡易な利用可能性ヒューリスティックを測定する 5 つの質問を行った結果（5 点満点）を図 7 に示している。どちらかというと想起しやすい物事の確率を高く見積もる傾向がたかい回答者が多いことがうかがえる（平均点は 1.8 点であった）。

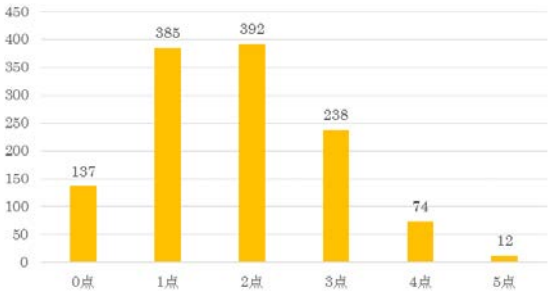


図 7：利用可能性ヒューリスティック

4 実証分析 - 炎上への参加メカニズム -

4-1 はじめに

昨今、ソーシャルメディアの普及に伴い、個人が容易にプライベートな情報を気楽に発信できる時代となった。その一方で、不謹慎・モラルに欠ける投稿を行った結果、「炎上」（Flaming）という社会問題が起こっていることは周知の事実である（伊地知; 2009）。これら炎上させた個人や企業の行動分析についてはいくつ

か行われているものの、その炎上の一躍を担っている炎上に加担している個人に注目している研究はこれまでほとんどない。例え不謹慎なソーシャルメディアへの投稿であったとしても、その投稿に対する批判的なコメントをした側も、その様態によっては法的責任を負う場合がある（永井; 2014）。例えば、その事実が真実であったとしても，公的な事項を公益目的で発信した場合を除き，基本的には名誉毀損に当たったり、プライバシーの侵害や著作権侵害に抵触したりすることもある。そして、その行動は個人の責任で済まず、所属組織の責任も問われかねないこともある。そう考えると、炎上させた個人だけでなく、炎上に参加（加担）する個人の存在も企業にとってはリスクの一つと考えることができる。そこで、本研究では、2014 年 3 月に竹村が実施したアンケート調査結果（個票データ）を用いて、炎上に加担する個人の特徴を明らかにし、マネジメントの観点から企業組織としてすべきことについて考察を行う。

本研究に用いる個票データは竹村が第 3 節で紹介したアンケート調査を実施する前に行っていた「2014 年労働者の情報セキュリティ意識等に関する調査」（2014 年 3 月にインターネット調査形式で実施）（以下、「2014 年労働者調査」と略する）から得られたものである。本調査は、 2 年以上同一の組織で働いている労働者（20 歳以上）を対象とし、彼ら・彼女たちのインターネット利用および情報セキュリティへの意識や行動等を把握するために行ったものである。質問項目としては、情報セキュリティ意識、情報セキュリティ行動、組織内で実施されている情報セキュリティ対策（技術およびマネジメントに関するものも含む）、職場環境、個人属性等、多岐に及んでいる。なお、（有効）回答者数は 1,507 人である。

4-2 調査概要

「2014 年労働者調査」において、日常の個人の行動の一つとして「他人のブログを炎上させることに参加すること」についての質問があり、「ない」と回答したのが 1,335 人（88.59%）、「何度かある」と回答したのが 117 人（7.76%）、「ときどきある」と回答したのが 49 人（3.25%）、「頻繁にある」と回答したのが 6 人（0.4%）という結果（図 7）となり、全体の約 11%の個人が少なくとも一度は他人のブログを炎上させることに参加した経験があることがわかる。上述したように、これらの個人も時として法的責任を負う場合があり、それは個人の責任で済まずに所属組織の責任も問われかねないこととなる。そう考えると、見落としがちではあるが、炎上に加担する個人の存在も企業にとってはリスク要因の一つとなり得る。

意識に関して、本調査でいくつかの質問をしている。その中で、本研究では、他人のブログを炎上させることに参加することへの抵抗感、コンプライアンス意識、セキュリティポリシー違反に対する意識や情報セキュリティ意識を取り上げる。例えば、他人のブログを炎上させることに参加することへの抵抗感について、「全く抵抗を感じない」と回答したのが 6 人（0.4%）、「あまり抵抗を感じない」と回答したのが 30 人（1.99%）、「どちらともいえない」と回答したのが 313 人（20.77%）、「やや抵抗を感じる」と回答したのが 381 人（25.28%）、「非常に抵抗を感じる」と回答したのが 777 人（51.56%）であり、多くの回答者がどちらかというと他人のブログを炎上させることに参加することに抵抗感を持っていることがわかる（図 8）。

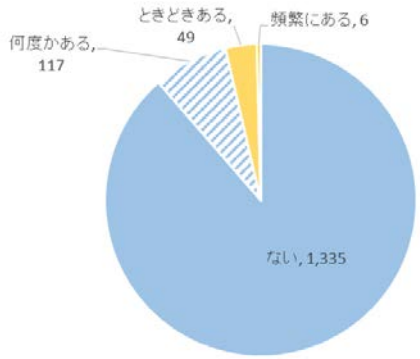


図 7: 他人のブログを炎上させることに参加した経験

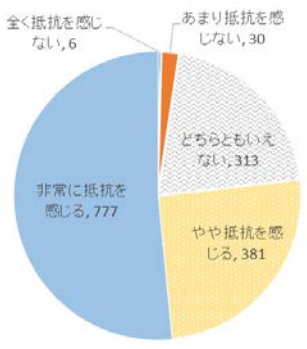


図 8: 他人のブログを炎上させることに参加することへの抵抗感

本研究では、組織環境として 2 つの側面を取り上げる。一つは職場において不正や違反が放置（黙認）されやすい環境であるかを表す不正・違反放置の職場環境という側面、もう一つは様々なルール導入の際、利用部門と意見交換を行ったり、幅広い人材の育成のために部署替え等を行ったりしているコミュニケーションを重視する職場環境という側面である。本調査では前者に関しては星野他（2008）で用いられている質問項

目の一部を採用している。

その他の属性としては、年齢、性別、職種、主観的な知識、ネット依存を取り上げた。主観的知識は、インターネットや IT に関する知識をどの程度持っているかを「平均的な人よりかなり知らない」から「平均的な人よりかなり知っている」の 5 段階で質問しており、この質問から、その個人がインターネットや IT に関する知識をもっているかの自信を表すものと本研究では考えている。また、ネット依存に関して、本調査では、藤（2011）のインターネット行動尺度の一つである「現実とバランスの側面」（没入的関与・依存的関与・非日常的関与）を質問項目として採用している。

4-3 分析結果

本研究では、他人のブログを炎上させることに参加するという行動にどのような要因が影響しているかを調べるために、2 項ロジットおよび多項ロジット分析を行った。分析モデルは図 9 に示した通りである。なお、質問項目の中でも単項目で回答を得ることで十分であると考えられるものは単項目指標のまま分析に用いているが、そうでないものについては PRIDIT 手法による指標の作成を行っている。なお、分析および分析結果の詳細については、竹村・花村（2014）を参照されたい。

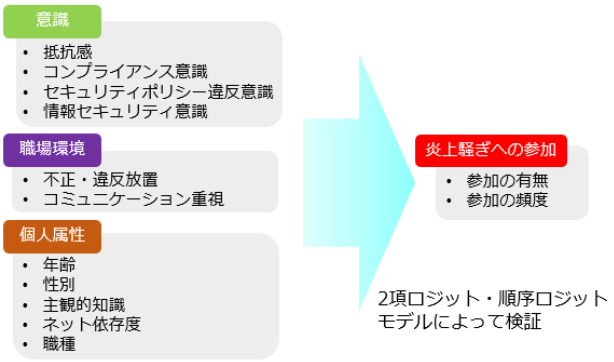


図 3：分析モデル

分析結果は表 2 と表 3 に示した通りである。表 2 および表 3 より、まず、意識に関して、抵抗感、コンプライアンス意識、情報セキュリティ意識の係数は 1%水準で有意となり、その符号はいずれも負の値をとっている。また、セキュリティポリシー違反意識の係数については表 2 では 10%水準、表 3 では 5%水準で有意となり、その符号は正の値をとっている。つまり、前者はいずれも意識を高めることによって、他人のブログを炎上させることに加担する行動（ある意味、不用意な行動）を抑止することにつながることがわかる。一方で、後者は違反意識・意図を低くすることで、この不用意な行動を抑止することにつながる。次に、職場環境に関して、不正・違反放置の係数は 1%水準で有意で正の値をとっている一方で、コミュニケーション重視の係数は表 2 では 10%、表 3 では 5%水準で有意となり、その値は負となっている。この結果は、不正や違反を放置する職場環境は、個人が不用意な行動を起こすことにつながり、一方で十分なコミュニケーション

表 2：分析結果 II（2 項ロジット分析）

	Coef.	Std. Err.	P>z	[95% Conf.	Interval]
抵抗感	−0.720	0.131	0.000	−0.976	−0.464
コンプライアンス意識、	−0.669	0.155	0.000	−0.972	−0.366
セキュリティポリシー違反意識	0.256	0.150	0.087	−0.037	0.549
情報セキュリティ意識	−0.830	0.162	0.000	−1.148	−0.512
不正・違反放置	1.285	0.166	0.000	0.960	1.610
コミュニケーション重視	−0.247	0.138	0.075	−0.518	0.025
年齢	−0.018	0.009	0.052	−0.035	0.000
性別	0.652	0.234	0.005	0.193	1.111
営業職ダミー	0.032	0.300	0.915	−0.557	0.621
事務職ダミー	−0.193	0.242	0.426	−0.668	0.282
主観的な知識	0.285	0.118	0.016	0.053	0.517
ネット依存	0.011	0.136	0.933	−0.255	0.277
_cons	−1.197	0.782	0.126	−2.729	0.335
Number of obs = 1507					
LR chi2(12) = 463.88 (Prob > chi2 = 0.00)					
Log likelihood = −303.152					
Pseudo R2 = 0.434					

表 3：分析結果 II（多項ロジット分析）

	Coef.	Std. Err.	P>z	[95% Conf.	Interval]
抵抗感	−0.753	0.128	0.000	−1.004	−0.502
コンプライアンス意識、	−0.629	0.151	0.000	−0.925	−0.334
セキュリティポリシー違反意識	0.312	0.145	0.031	0.028	0.596
情報セキュリティ意識	−0.707	0.159	0.000	−1.019	−0.394
不正・違反放置	1.412	0.168	0.000	1.083	1.742
コミュニケーション重視	−0.310	0.135	0.022	−0.575	−0.045
年齢	−0.013	0.008	0.137	−0.029	0.004
性別	0.520	0.226	0.022	0.076	0.963
営業職ダミー	−0.054	0.283	0.848	−0.609	0.500
事務職ダミー	−0.243	0.233	0.297	−0.699	0.214
主観的な知識	0.286	0.115	0.013	0.061	0.512
ネット依存	0.065	0.134	0.625	−0.197	0.328
/cut1	1.186	0.758		−0.301	2.672
/cut2	2.902	0.768		1.396	4.408
/cut3	5.403	0.858		3.722	7.084
Number of obs = 1507					
LR chi2(12) = 475.5 (Prob > chi2 = 0.00)					
Log likelihood = −424.088					
Pseudo R2 =0.359					

を取ることができる職場はそのような行動を抑止することにつながることを意味している。これらの結果は、直感的にも正しいように思える。

さらに、個人属性について見てみると、年齢の係数は表 2 では 5%水準で有意となり、その値は負となっている（表 3 では有意となっていない）。性別に関してはいずれも少なくとも 5%水準で有意となり、その値は正となっている。職種ダミー（営業職、事務職）の係数およびネット依存の係数に関してはいずれの結果でも統計的に有意ではなかった。主観的な知識はいずれの表においても 5%水準で有意となり、正の値をとっている。炎上させている個人は若者（若年層）が多いと言われているが、他人のブログを炎上させる行動をとっている個人も、2 項ロジット分析の結果から、同じ傾向があると読み取れる。また、ネットへの依存が高いほど、このような行動をとると思われがちであるが、少なくとも今回の調査からは、必ずしもネット依存が高いからといって不用意な行動をとるとは言えないことがわかる。分析結果から主観的な知識が高い（よりインターネットや IT に関する知識をもっている自信がある）ほど、不用意な行動をとる傾向があると読み取れる。言い換えると、自信家であるほど、そのような行動を取りやすいとも言える。ただし、本調査では、客観的な知識ではなく、主観的な知識を問うているために、インターネットや IT に関する知識を持っている個人ほど、そのような行動をとることを意味していないことに注意されたい。

4-4 まとめ

他人のブログを炎上させることに加担する行動は、個人の意識の問題であると同時に、その個人が所属する組織の環境からも影響を受けることが分析の結果からわかった。炎上を引き起こす個人に対する対策として、組織人としての教育、個人ユーザのモラル向上、SNS 利用ポリシーの規定などが考えられるが（情報処理推進機構, 2014）、これは本研究で取り上げた他人のブログを炎上させることに加担する個人に対しても当てはまる。そのため、モラル向上、組織人としての教育を行い、そのような不用意な行動を行わないこと、また不用意な行動が組織に損害を招く可能性があることを周知しておく必要がある。

5 おわりに

本調査研究では、アンケート調査から SNS ユーザのインターネット上での行動やセキュリティ意識、プライバシー意識の把握等の把握を行った。また、竹村が過去に収集・蓄積されたデータを用いて彼らのネット上での行動、とりわけ炎上への参加メカニズムについて分析を行った。現状把握および実証分析については、すでに上述した通りである。その実証分析では、労働者（社会人）のみを対象としてその行動メカニズムを見てきたが、本調査研究では社会人のみならず、学生や主婦・主夫が含まれている。そのため、今後、本調査研究で収集・蓄積したデータを用いて、更なる分析が可能となる。また、最初に述べたように、セキュリティエコノミックスの分野はまだ萌芽状態にあるために、このデータの一部を、回答者（個人）を特定できる情報を除いた形で学術研究目的の利用者（国内外）に限定して提供していく予定である [6]。さらに、今後この学術分野を深化させていきたいと思う。

【参考文献】

Cass, R.S. (2001) Republic.com, Princeton University Press, (2001).

Joinson, A.N. (2003) Understanding the Psychology of Internet Behavior: Virtual Worlds, Real Lives, Palgrave Macmillan.

Kotulic, A.G., Clark, J.G. (2004) Why There Aren't More Information Security Research Studies, Information and Management, Vol.41, pp597-607.

Takemura, T. (2011) Empirical Analysis of Behavior on Information Security, Proceeding of 2011 IEEE International Conferences on Internet of Things, and Cyber, Physical and Social Computing, pp358-363.

石田浩・佐藤香・佐藤博樹・豊田義博・萩原牧子・萩原雅之・本多則惠・前田幸男・三輪哲 (2009)「信頼できるインターネット調査法の確立に向けて」『SSJDA リサーチペーパーシリーズ』, No.42.

伊地知晋一 (2009)『ネット炎上であなたの会社が潰れる!』, WAVE 出版.

大隅昇 (2006)「インターネット調査の抱える課題と今後の展開」『ESTRELA』, No.143, pp2-11.

キンバリー・ヤング (1998)『インターネット中毒～まじめな警告です』(小田嶋由美子 訳), 毎日新聞社.

情報処理推進機構（2015）「2014 年度情報セキュリティの倫理に対する意識調査報告書」
http://www.ipa.go.jp/files/000044094.pdf.
星野崇宏（2009）『調査観察データの統計科学―因果推論・選択バイアス・データ融合』岩波書店.
星野崇宏・荒井一博・平野茂美・柳澤秀吉（2008）「組織風土と不祥事に関する実証分析」『一橋経済学』, Vol.2, No.2, pp157-177.
竹村敏彦・花村憲一（2014）「ネット炎上に加担する個人属性に関する考察」『第 69 回日本情報経営学会予稿集』, pp127-130.
田代光輝（2012）「大学生のネット炎上分析と予防及び対応の提案: 好ターゲットとしての大学生の実情とネット炎上からの回避の提案」『大妻女子大学紀要』, No.21, 233-241
辻大介（2008）「インターネットにおける「右傾化」現象に関する実証研究: 調査結果概要報告書」
http://www.d-tsuji.com/paper/r04/index.htm.
永井徳人（2014）「ソーシャルメディアをめぐる動向とリスク管理」『情報教育資料』, No.38, pp8-11.
藤桂（2011）「インターネット行動尺度」吉田富二雄・宮本聡介（編）『心理測定尺度集 V: 個人から社会へ＜自己・対人関係・価値観＞』, pp294-302.
三浦麻子・森尾博昭・川浦康至（2009）『インターネット心理学のフロンティア-個人・集団・社会』, 誠信書房.
労働政策研究・研修機構（2005）「インターネット調査は社会調査に利用できるか」『労働政策研究報告書』, No.17.

1) Cass (2001)で提唱されたインターネット上の集団極性化であるサイバーカスケード（cyber cascade）の 1 つである。
2) インターネット調査には、ウェブサイトを開設しそこで不特定多数を対象にアンケートを実施する「オープン型」とモニターパネル（ポータルサイトやアフィリエイトプログラムを通じてアンケートに協力してくれる回答者）などを利用し彼らの情報を基にサンプリングを行ってアンケートを実施する「クローズ型」があり、本調査は後者を採用した（大隅; 2006）。
3) アンケート調査票を近日中に竹村研究室のウェブサイト URL＜http://ecolab.eco.saga-u.ac.jp/inf_sec/＞にて公開予定である。
4) 本調査では、サービス名ごとに悪意ある投稿について質問しているが、ここではサービス名を問わずに投稿経験があるかをまとめたものとしている。
5) 国内では、独立行政法人国立病院機構久里浜医療センターがウェブサイト＜http://www.kurihama-med.jp/tiar/tiar_07.html＞に IAT を翻訳し公開している。
6) 竹村研究室のウェブサイト＜http://ecolab.eco.saga-u.ac.jp/＞にてその利用方法等を紹介している。

〈発　表　資　料〉

題　　名	掲載誌・学会名等	発表年月
我が国のクラウドコンピューティング・ ビックデータの利活用の現状について	第 68 回日本情報経営学会（大正大学）	2014 年 5 月
クラウドコンピューティングの普及が我が国のマクロ経済に与える影響	第 31 回情報通信学会（大阪大学）	2014 年 6 月
ネット炎上に加担する個人属性に関する考察	第69回日本情報経営学会全国大会（ホテル日航八重山）	2014 年 11 月