

## ソーシャルコンピューティング可視化サービスの検討

橋本 隆子<sup>†1</sup> 白田 由香利<sup>†2</sup>

ネットワーク網が成熟した情報社会において、ブログや SNS といったソーシャルコンピューティングサービスの普及が目覚ましい。ソーシャルコンピューティングサービスでは、不特定多数の利用者によるオンラインの議論やコミュニケーション（以下、サイバー議論と記す）が数多く行われており、プライバシー情報の漏えいや他人への誹謗中傷といったトラブルが発生している。結果として議論が「炎上」したり、取り返しのつかない事態に陥ってしまうこともあり、近年大きな社会問題となっている。これらの課題を解決するためには、さまざまな情報技術を統合したソリューションが必要となる。本稿ではソーシャルコンピューティングにおけるトラブルの例を挙げ、特にサイバー議論における「炎上」に注目し、その度合いを検知する手法について検討を行い、それを活用したソーシャルコンピューティング可視化サービスの提案を行う。

### Social Computing Visualization Service

TAKAKO HASHIMOTO<sup>†1</sup> and YUKARI SHIROTA<sup>†2</sup>

In the advanced information network society, social-computing that has various cyber-discussions is confronting different problems such as leakage of personal information, cyberbullying. To solve the issues, the solution using appropriate information technologies would be needed. In this paper, we give examples of issues in social computing. We also consider method to detect the degree of the "blog under fire," and propose effective solutions on the social computing visualization service.

<sup>†1</sup> 千葉商科大学  
Chiba University of Commerce

<sup>†2</sup> 学習院大学  
Gakushuin University

### 1. はじめに

ネットワーク網が成熟した情報社会においては、人々がコミュニケーションを取り合い、情報を共有しあうことができるソーシャルコンピューティングサービスの普及が目覚ましい。ブログや SNS といったソーシャルコンピューティングサービスでは、不特定多数の利用者によるオンラインの議論やコミュニケーション（以下、サイバー議論と記す）が行われており、他人への誹謗中傷、プライバシー情報の漏えいといったトラブルが発生している。結果として議論が「炎上」してしまい、サイバー掲示板が閉鎖されてしまう事態も多々見られている。ソーシャルコンピューティングサービスの利用者が、被害者だけでなく、無意識のうちに加害者となってしまう事例も報告されており、近年大きな社会問題となっている。

このような問題を防ぐためには、ソーシャルコンピューティングサービスの利用者一人ひとりにインターネットを利用する際のルールやマナー（ネチケット）を啓蒙することが必要である。それに加えて、情報技術を活用した問題解決のソリューションを実現することもまた重要となると考える。

本稿では、ソーシャルコンピューティングサービスにおけるトラブルの例を挙げ、利用者を取り巻く今と昔の環境の違いについて考察する。それを踏まえ、サイバー議論の状況を把握し、議論の「炎上」の度合いを検知するための手法について検討を行う。本手法は既存の情報技術の統合であり、ソーシャルコンピューティングで発生するさまざまな課題を解決するための最初のステップとなると我々は考える。さらに提案手法に基づいたソーシャルコンピューティング可視化サービスの提案を行う。

### 2. ソーシャルコンピューティングサービスにおけるトラブル

表 1 はソーシャルコンピューティングサービスで発生しているトラブル例を記載したものである。以下、表 1 を参照しながら、議論を進める。

#### (1) プライバシー情報の漏えい

プライバシー情報の漏えいは、掲示板、ブログ、SNS、そして「プロフ」と呼ばれる個人情報交換サービスなどで問題となる。プロフとは携帯電話や PC のサイト上に自己紹介を掲載し、会員同士が ID を交換し合ったり、サイト内を検索することで見つけた相手の掲示板に書き込みをし、コミュニケーションをとるといったサービスである。女子中高生を中心に爆

表 1 ソーシャルコンピューティングサービスにおけるトラブル例  
Table 1 Cyber-community risks: examples, and environments of old and now.

	(1) プライバシー情報漏えい	(2) 他人への誹謗中傷	(3) 炎上	(4) 匿名・チェーンメール	(5) 出会い系サイト	(6) 不適切サイト
トラブル例	・インターネット掲示板で、イニシャルを使って、人物を特定できる内容で書き込み。 ・下着姿の写真をブログにアップしたところ、自由にコピーされ、改変など悪用される	・学校裏サイトなどで、友人・教師などへの誹謗中傷。 ・ネット上で誹謗中傷が加速すると、それにつれて実生活でも、いじめが広がる。	・特定の書き込み（または書き込みをした人）に対して、批判的なコメントが殺到。 ・炎上に管理者が耐えられなくなり、サービスを閉鎖してしまう。	・匿名メールを出して、友人に嫌がらせ。 ・友達の携帯やサブアドレスを使って、成りすましメール。	・出会い系サイトに、援助交際を求める書き込み。 ・出会い系サイトで相手を知ったつもりになって、実際に会い、犯罪に巻き込まれる。	・気づかないうちに、悪質なサイトにアクセスしてしまう。 ・メールなどに書かれているサイトのアドレスをクリックしただけで、不当に料金を請求される（ワンクリック請求）

発的な広まりを見せており、700万人を超す利用者を有するサイトもある<sup>1)</sup>。このプロフにおいては、約2割の利用者が本名由来のハンドルネームを使用し、9割以上の利用者が性別を公表、小中学生の利用者の3割がコンタクト先としてメールアドレスを登録しているといった報告もある<sup>2)</sup>。掲示板やブログにおいても、自らの個人情報無防備に記載する例などが報告されている<sup>3)</sup>。これらの情報及び情報の組み合わせにより、プライバシー情報が判明し、本人への到達が可能となるといった事例も確認されている。

## (2) 他人への誹謗中傷

掲示板やSNS上で他人への批判や非難を書きこむ現象もよく見られている。ネット上で他人を誹謗中傷したり、悪質な書き込みをしたりすることは名誉毀損罪といった犯罪ともなり、ソーシャルコンピューティングサービスの利用者が無意識の内に加害者となってしまう事例の一つと言える。

## (3) 炎上

ブログやSNSに投稿された特定の書き込みに対して、批判的なコメントや不適切な書き込みが殺到する状況が「炎上」である。上記(2)の他人への誹謗中傷の延長にあるとも言える。誹謗中傷が特定の個人へ集中すると、いわゆる「ネットいじめ」となる。若年層におけるネットいじめは、現実の人間関係に影響を及ぼす傾向にあり、ネット上の関係と現実社会の人間関係の相乗効果によりいじめが加速して、一層大きなトラブルとなる事例も発生している<sup>4)</sup>。もちろん炎上にもさまざまなレベルがあり、炎上しても比較的すぐ沈静化する場合と、書き込み増加によるサーバーの負荷増大や見るに堪えない(場合によっては犯罪ともなる)不適切な書き込みの連続に管理者が耐えられなくなり、サービスの閉鎖に至る場合など

がある。管理者がサイバー議論の状況を把握し、できるだけ素早く適切な対応をとることが重要といわれている<sup>5)</sup>。

この他、(4)匿名メール・チェーンメール、(5)出会い系サイト、(6)不適切サイトなど、ソーシャルコンピューティングサービスにはさまざまなトラブルが発生している。

情報社会到来以前の社会では、対面によるコミュニケーションが主であり、遠隔の相手とのコミュニケーション手段は主に手紙や電話であった。情報の伝達は紙ベースであり、複写・印刷しなければ大量の情報配布はできなかった。口頭での情報伝達は記録に残りにくく、失言等があっても忘れられていく傾向にあった。

一方、過去の社会と比較すると、現代の情報社会には以下のような特徴がある。

### ● メリット

- (1) 一度インターネットに配信したデータは広く公開される
- (2) いつでもどこでもインターネットにアクセスできる
- (3) 見知らぬ人とも気楽にインターネット上で出会うことができる
- (4) 簡単にアカウントを作成できる

### ● デメリット

- (1) 身分の査証が容易であり、匿名性があると誤解しやすい
- (2) 閉じたコミュニケーションになりやすい
- (3) 文字によるやりとりで感情が伝わりにくく、誤解を生みやすい

上記のような特徴から、利用者は情報社会に潜むリスクに気付くことなく、安易にソー

シャルコンピューティングサービスを利用してしまふ。その結果として前述のようなトラブルに遭遇してしまうといえる。このような情報社会においては、ソーシャルコンピューティングサービスで発生するトラブルをできるだけ早期に検知し、適切に対応を行っていく取り組みが重要となると考える。

我々は、情報技術を活用することで前述のようなさまざまなトラブルから利用者を守る「技術の仕組み(基盤)」を提案していくことを目指し、その検討を行っている。情報技術にはプライバシー検知技術、コミュニティ解析技術など種々の技術があるが、これらの技術は必ずしも現実のトラブル解決に十分に活用されていない。

たとえばブログ、SNS、プロフなどでは、利用者は一定の対策をとりつつ、個人情報の開示を行っているとの調査がある<sup>2)</sup>。しかしながら、利用者が小出しで開示した個人情報を組み合わせることで本人を特定できてしまう場合も見られる。こういったリスクを避けるために、プライバシー情報を検知する技術の提案がなされている<sup>6)</sup>。この技術はプライバシー情報を表現する言葉を予め定義しておき、書き込みがその言葉を含んでいるかどうかを判断して、別な書き込みに記載されている情報と統合してプライバシー情報を検知するものである。ブログや SNS の書き込み情報を全て監視しておくことは難しく、効率的に検知する仕組みが必要となる<sup>7)</sup>。また、掲示板や SNS において、どういったメンバーが何回発言し、どのような議論がなされているか、などを可視化する技術もある<sup>8)</sup>。しかしながら、議論の推移を可視化するだけでは、それがトラブルとなりそうな議論なのか、何か対策を打つべき議論なのかなどを判断することは難しい。

さらにコミュニケーションの急な変化を知るための技術として、Kleinberg が提案している活性度検出手法<sup>9)</sup>がある。本手法は新聞記事などの時間情報のついた文書の集合をドキュメントストリームとしてとらえ、その中でドキュメント数が急激に増加している部分を発見する手法である。本手法をブログの解析に適用することで、議論が活性化したことを捉えることは可能となるが、それがトラブルに発展するか否かまで判断することはまた難しい。

このように、一つ一つの技術は限られた条件のもとでそれなりの精度を出せていても、実社会の課題に対して満足のいく有効性を発揮できるかといえば、必ずしもそうとは限らない。それぞれの技術は単独でなく、統合されてこそより現実的かつ効果的に動作すると考える。そこで我々は、既存の情報技術を現実に即した形で統合しながら、有効かつ効率的な解決策(ソリューション)を検討していきたいと考えている。本稿ではその第一歩として、サイバー議論の状況の可視化に焦点をあて、特に「炎上」している議論の特徴を考察することでソーシャルコンピューティングのトラブルをできるだけ早く発見する方法について議論し

ていく。

### 3. ソーシャルコンピューティングにおけるサイバー議論の状況

ソーシャルコンピューティングにおけるサイバー議論で発生するトラブルの解決のためには、サイバー議論の状況を何らかの形で獲得する手法が必要となると考える。本章では、ブログや SNS、匿名掲示板で行われているサイバー議論に関して、いわゆる「炎上」している状況を如何に早期に発見するかについて議論する。サイバー議論の炎上の早期発見は、ソーシャルコンピューティングサービスの利用者にとってもサービスの管理者にとっても、有用性が高いと考える。

#### 3.1 サイバー議論の炎上

本節ではサイバー議論の炎上について考察を行う。前章でも述べたとおり、サイバー議論がどの程度炎上しているか、管理者が何らかの対策を打つ必要があるかといったことを一目で判断するのは困難である。その一方でソーシャルコンピューティングサービスには数多くのサイバー議論が発生しており、議論の炎上の様子を判断するために、議論を一つ一つ手でチェックしていくのでは管理者の負担が大きくなりすぎる。

我々は予備実験として、実際の電子掲示板上<sup>10)</sup>で行われた 6 つのサイバー議論に対して、その書き込みの状況を調査し、友好的に行われたと思われる議論と、いわゆる炎上したと思われる議論の比較を行った。

図 1 は調査を行った 6 つのサイバー議論の書き込み数の推移を示したものである。議論開始から 48 時間以内の書き込みに関して、30 分ごとにその件数をカウントしグラフ化した。グラフの横に記載している は議論の炎上の度合いを示している。 が 3 つの時がもっとも炎上しており、以下 が少なくなるにつれて炎上の度合いが小さくなる。なお議論が炎上しているか否かは、本予備実験では筆者らが判定を行った。

さらに各サイバー議論に関し、以下の数値の測定を行った。

- 投稿数  $n$  : 一定期間  $w$  における書き込みの数
- 投稿頻度 : 書き込みの頻度情報.  $w/n$
- 投稿者数  $m$  : ある一定期間  $w$  におけるサイバー議論にコメントを書きこんでいる利用者数
- 一人当たりの平均投稿数  $n/m$  : 一人当たりの書き込み数。投稿数が多く、投稿者のばらつきが小さいと値が大きくなる。

ここでは  $w = 48$  時間として上記数値の測定を行った。その結果を表 1 に示す。

表 2 サイバー議論の状況 (議論開始 48 時間)  
Table 2 Cyber-community risks: examples, and environments of old and now.

ID	URL・概要	書き込み数 n	書き込み間隔 (48 時間 /n)	投稿者数 m	一人当たりの平均投稿数 n/m	フレーミングの書き込み状況	炎上の度合い
1	ネイルに関する議論 <sup>11)</sup>	146	0:19:44	71	2.06	「あなたが気持ち悪い」「臭い」などの書き込み多数あり	
2	差別に関する議論 <sup>12)</sup>	57	0:50:32	31	1.84	「偏見の持ち主」, 「人権侵害」などの書き込みあり	
3	近所付き合いに関する議論 <sup>13)</sup>	50	0:40:00	69	1.44	「気の毒」「わかります」などの共感の書き込みあり	
4	公立と私立学校の意識に関する議論 <sup>14)</sup>	46	1:02:37	38	1.21	スレ主に反論する書き込みは多数だが, 誹謗中傷の言葉ではない	
5	学歴コンプレックスに関する議論 <sup>15)</sup>	86	0:33:29	69	1.25	スレ主を励ます書き込み多数	
6	誕生日の過ごし方に関する議論 <sup>16)</sup>	52	0:55:23	44	1.18	スレ主を励ます書き込み多数	

一般に、書き込み頻度が急激に高まり、かつ人を誹謗中傷する言葉が見られる場合に、サイバー議論は炎上する可能性が高いと考える。特に炎上した議論では、特定の書き手に対して集中的に攻撃するような書き込みが見られる傾向がある。その一方で、書き込み頻度が急に高まり、あたかも炎上しているかのように思われる議論であっても、実際は有効な議論が行われているということもある。友好的な議論の場合は、たとえ書き手を攻撃するような意見が一部に見られたとしても、それを取りなしたりする中立的な書き込みが見られ、批判的な書き込みが集中することはないように見える。

実際に炎上したと判断できる図 1-1 の議論のグラフとそれ以外の議論の書き込み頻度を比較してみる。図 1-1 は 48 時間の間に 146 件の書き込みがあり、明らかに書き込み頻度が高い。さらに図 1-1 の実際の書き込みを見てみると、「不潔」や「気持ち悪い」といった人を誹謗中傷する言葉が見られている。一方、たとえば図 1-2 の書き込みには「偏見の持ち主」や「人権侵害」といった言葉が見られ、書き込み頻度が高まることがあるが、その都度議論の仲裁をする書き込みが現れ、落ち着いた状況を取り戻している。また図 1-3 の議論は、議論

開始当初に書き込み頻度が高まり炎上するかに見えたが、その後書き込み頻度はおさまり、友好的議論となっている。

ソーシャルコンピューティングサービスの管理者にとって、図 1-1 のような炎上するリスクの高い議論を早期に発見できれば有効である。またソーシャルコンピューティングサービスの利用者にとっても、自分が参加しようとしている議論の炎上の状況を知ることができれば、参加するサイバー議論の選択などに役に立つと思われる。

### 3.2 サイバー議論の炎上の可視化

前節の予備実験から、高い投稿頻度を持ち、相手を非難する(フレーミング)の書き込みが多く見られるサイバー議論が炎上するリスクが高いと予想できる。

我々はサイバー議論における書き込みの推移は正規分布でモデル化可能であると考え、ある一定の標準偏差、ピーク値を持つ正規分布の時に、その議論は炎上していると考えることができると予想する。実際に図 1-1 のサイバー議論の場合、図 2 で示すような正規分布でモデル化することができる。図 1-1 のサイバー議論においては、特に最初の山が大きく、

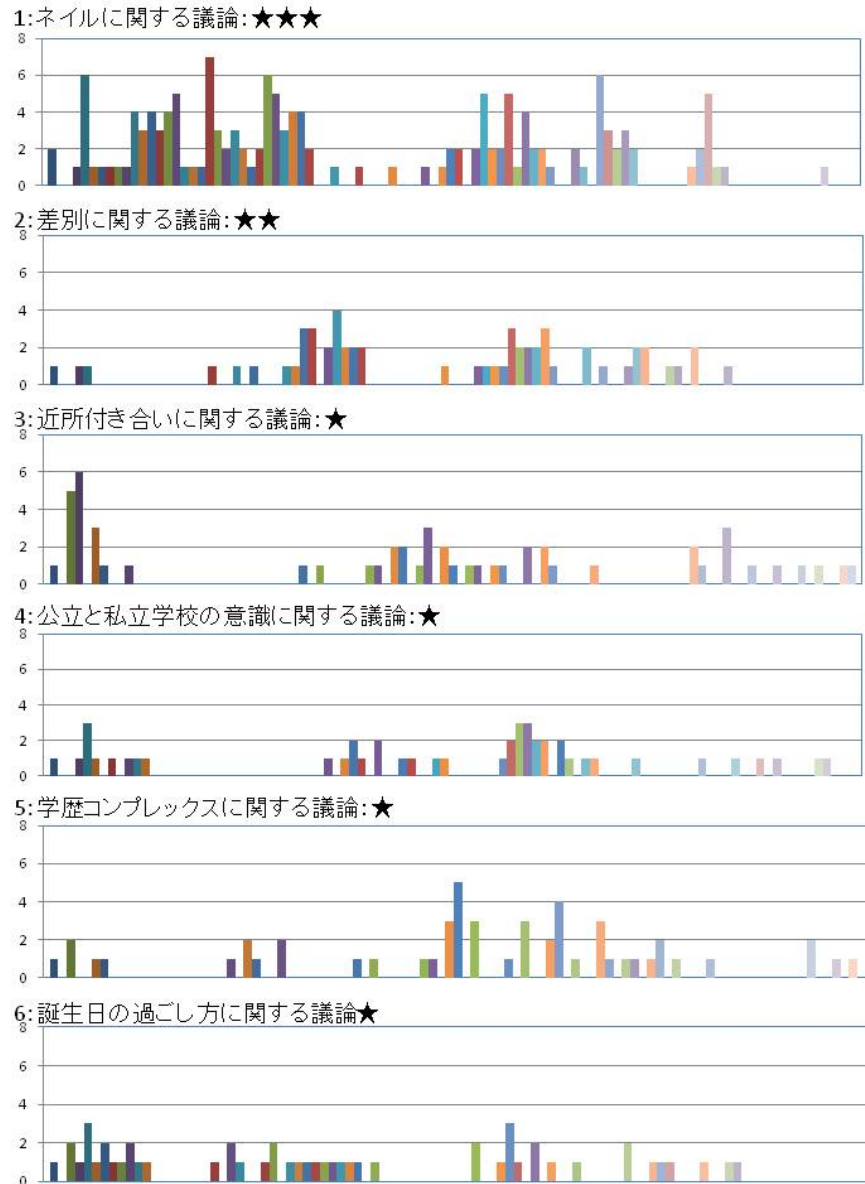
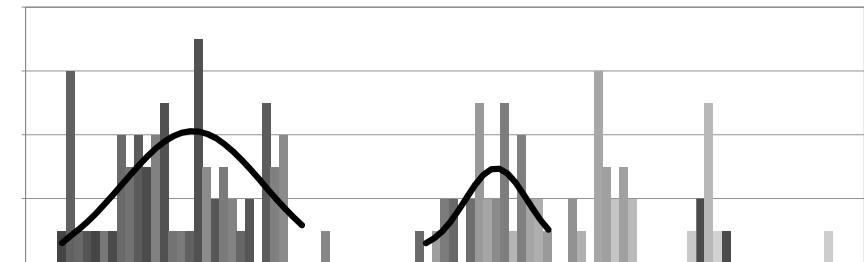


図 1 サイバー議論の投稿状況  
Fig.1 Solution conceptual diagram.



平均	2.48	2.00
標準偏差	1.63	1.50
ピーク値	3.96	3.33

図 2 炎上した議論の正規分布によるモデル化  
Fig.2 Solution conceptual diagram.

そこで議論の炎上が起きていると考えられる。もちろん正規分布の形のみで炎上を判断するのは前章で述べたように不十分な可能性があり、それを補う情報として、フレーミングの書き込みの有無、プライバシー情報の漏えいの有無などを自然言語処理技術（フレーミング言語の検知）、プライバシー情報検知技術などを利用して抽出することが必要となる。これらの技術を統合することで、将来的には炎上のリスクを数値化し、可視化できる技術基盤を構築したいと我々は考えている。

今回の予備実験ではフレーミングの書き込みの判断を手作業で行ったが、今後は自然言語処理技術を統合することで、自動的に判断していくことを検討し、炎上のリスクの数値化を試みていく。

#### 4. ソーシャルコンピューティング可視化サービス

##### 4.1 システムの概要

図 3 は、我々が提案するシステムの概要図である。本システムはさまざまな技術の統合により構築され、サイバー議論の状況を可視化する。

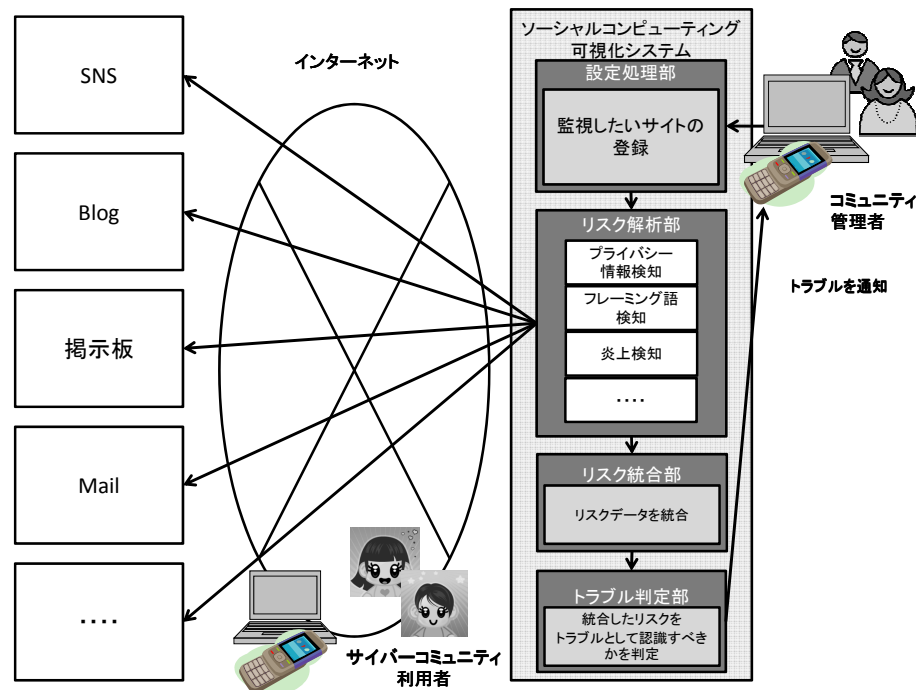


図 3 システム概要図  
Fig. 3 Solution conceptual diagram.

ソーシャルコンピューティングサービスの管理者は、トラブルを検知したい(監視したい)サイバー議論の URL を登録する(設定処理部)。技術統合部は設定処理部で登録されたサイバー議論の URL からその議論の状況を解析し、解析に必要なデータの抽出を行う。抽出されたデータはサイバー議論の状況を解析するリスク解析部内の各技術(プライバシー検知技術、炎上検知(活性度検出)技術、フレーミング言語検知(自然言語処理)技術など)のインプットとなる。各技術はインプットデータを基に炎上のリスクを算出する。このリスク解析部はさまざまな技術を集めて構成される処理部である。それぞれの技術の観点からリスクの数値化を行う。リスク統合部は、リスク解析部の各技術により導出された炎上のリスク(数値)を統合し、統合リスクとする。トラブル判定部は、統合されたリスクがトラブルとして認識できるかを判定する。トラブルとして認識された場合、統合リスクの情報を可視化し、コミュニティ管理者へ通知を行う。

## 5. ま と め

情報技術を実社会で真に活用することを目的として、ソーシャルコンピューティングにおける課題解決の仕組みについて考察を行った。今回は特にサイバー議論の炎上に注目し、投稿状況を正規分布で可視化することで、炎上を検知できるかについて検討を行った。今後は、ソーシャルコンピューティングの課題とその解決策に関して、フィールドリサーチも含めて考察を重ねていく。特にソーシャルコンピューティングサービス上で発生するさまざまなリスクの定義、リスクを検知するために必要なデータ、トラブルとして認識するための条件、可視化手法について考察を行っていく予定である。システムアーキテクチャについても考察を重ね、ソリューションのために必要な情報技術を体系化し、その統合に向けた検討を行っていきたいと考えている。

## 参 考 文 献

- 1) 前略プロフィール, 楽天, <http://pr.cgiboy.com/>.
- 2) 佐藤元彦ほか: プロフの現状・青少年の危機意識について, JSSM 第 23 回全国大会研究報告書, pp.153-156 (2009).
- 3) 子供たちのインターネット利用について考える研究会:第一期 報告書 (2008).
- 4) 荻上チキ: ネットいじめ ネット社会と終わりなき「キャラ戦争」, PHP 新書 (2008).
- 5) 伊地知晋一: 実例に学ぶ ブログ炎上, [http://ascii.jp/elem/000/000/425/425681/\(2007\)](http://ascii.jp/elem/000/000/425/425681/(2007)).

- 6) 渡辺夏樹ほか：自然言語文からのプライバシー情報検知システム -自然言語情報の開示制御技術 DCNL の実現 (1) -, 研究報告「コンピュータセキュリティ (CSEC)」, No.2009-CSEC-044 (2009) .
  - 7) Nanno T., Fujiki T., Suzuki Y., and Okumura M.: *Automatically collecting, monitoring, and mining japanese weblogs*, In Poster Session of the 13th International World Wide Web Conference(2004).
  - 8) 松村 真宏ほか：議論構造の可視化による論点の発見と理解，知能と情報：日本知能情報フアジィ学会誌 (2003).
  - 9) Kleinberg, J.: *Bursty and Hierarchical Structure in Streams*, AProceedings of the Eighth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining,pp.91-101(2002).
  - 10) インターエデュ , <http://www.inter-edu.com/>.
  - 11) <http://www.inter-edu.com/forum/read.php?1279,1347420>.
  - 12) <http://www.inter-edu.com/forum/read.php?1277,1386075>.
  - 13) <http://www.inter-edu.com/forum/read.php?1279,1433640>.
  - 14) <http://www.inter-edu.com/forum/read.php?1279,1433662>.
  - 15) <http://www.inter-edu.com/forum/read.php?1277,1421043>.
  - 16) <http://www.inter-edu.com/forum/read.php?1277,1418729>.
-