

SNS 炎上による会社のリスクとマニュアル整備

1160461 板東 亮佑

高知工科大学マネジメント学部

1. 概要

これまで会社はリスクリテラシーを学び、リスクの影響する範囲を小さくすることで、自身に起こりうる危機を回避してきた。しかし、様々な技術や機器の誕生によって、リスクの影響する範囲は拡大し、今までより広い範囲において危機管理への対策が必要になった。そこで本研究では SNS の使用という新たに生まれたリスクの影響と、対応策について考察する。そのためにリスクリテラシーの視点から、SNS がどのような影響を及ぼすのか、SNS 炎上の事例からどんな時に会社自体に影響を及ぼすのか、またどんな層が影響を及ぼしやすいのかを調査し、SNS に対する対策を提案する。

1.1 研究の背景

近年のスマートフォンの普及により、ますますインターネット人口が増加している。その中で SNS の使用率も若い年代を中心に増加の傾向にある。それに伴って、近年 SNS に関する事件が増加している。会社の従業員がプライベートで SNS を使用することにより、その社員が属する会社への評価や信頼を落とす行為へとつながる事件が多発している。新しいリスクの一つとして SNS の使用が認識されている。

1.2 研究の目的

SNS の使用が新たな会社のリスクとして認識され始めたことで、どのような影響がどの範囲まで及ぶのかを考える必要がある。リスク管理において、SNS の使用リスクを含め、問題が発生した際にどう対応していくのかを考える。SNS の炎上がどんな年代やどんな状況によって発生してきたかを調査する。そのことから未然の対応策、すなわち、ど

のような対応によって事件数を低減することが出来るかを明らかにする。

1.3 本論文の構成

研究方法からはリスクリテラシーの面から SNS 使用の影響力や顕在化状態を調査する。その際にリスクリテラシーの説明を行う。それと併せて SNS の使用率とインターネットの普及率なども示す。実際の事例から、それらはどのような事件だったのか、そこからわかること、並びに、リスク管理の問題として捉えられることを述べる。次に、事例とリスクリテラシーの関係について述べ、SNS の問題として何が問題の本質なのかを把握し、その問題への解決策を提示する。その問題を解決するためにマニュアルや事後の対応についての評価を行う。最後に、結論を述べる。

2. 研究方法

この研究で必要になるリスクの観点、リスクリテラシーについてまず述べる。

リスクリテラシーとは、リスクマネジメントの体制に、基本的な考え方は別に新たな概念を導入し、高度なものとするものである。その概念をリスクリテラシーとする。リスクマネジメントの基本的な考え方は五段階に分けられる。それは

(1) トップの理解とリスクビジョン、(2) リスク対策本部の設置とリスクマネージャーの養成、(3) リスクマニュアルの作成、(4) リスクマネジメントの訓練と実践、(5) リスクコミュニケーション手法の確立とウェブ戦略である。次章では、林 志行氏の現代リスクの基礎知識 事例で学ぶリスクリテラシー入門の記述に基づいて、研究に関わりのある部分を述べる。

3. リスクリテラシーの理論

(1) のトップの理解ではリスクマネジメントの実施の宣言を経営トップ自らが行うことが大事である。これは全社に対して、これから設置するリスク対策本部の意義やリスクマネージャーの権威などをわかりやすく「社内に公開する」ことである。この「社内に公開する」というのは経営トップとして権限を認めていることを示せば十分である。その意味としてリスク管理部門の最高責任者に副社長や常務クラスを置くことが一般的である。端的に言えば、物理的コストを機動的に動かせる体制を整備することを意味する。

リスクビジョンではリスクマネジメントをどういう範囲で行うのか、リスク対策本部の特性を決める必要がある。企業経営全般に対してコメントできる立場にするのであれば、「マネジメント」に重点を置き、直接的な事件・事故に対応し、事前予防を中心とする場合は、「リスク」にアクセントが来る。

リスクには定量的なものだけでなく、定性的なものも含まれる。地震や工場の爆発、不良品の回収、謝罪と姿形のわかりやすいものだけでなく、ネット犯罪、従業員の不正、自社ブランドのイメージの低下なども企業が抱えるリスクに含まれる。このリスクのどのレベルまでを自社のマネジメントレベルとするか、誰がマネジメントを行うのかを決定することが求められる。これは結果的に、経営層がどこまで受け入れるかに関する経営判断となり、リスクとマネジメントのどこで線引きするかという経営戦略上の問題に帰着する。多くの企業でリスクマネジメントが機能しないのは、経営レベルでの組織内部の軋轢、リスク対策本部やリスク対策室で吸収、発散できないためである。その二つを理解した上で次に、どの程度リスクを回避し、どこに企業としての脆弱性が存在するかの分析が必要となる。「リスク回避度」は自社がどの程度のリス

クを持ち、その結果どの程度の期待(リターン)を必要としているかを表す指標である。「リスク許容度」は、リスク毎にどの程度まで持ちこたえることが出来るかを表す指標である。その分析は、直接的なリスクだけでなく、間接的なリスクについての自社のスキル、潜在的なパフォーマンスを検証することである。こうした事柄は、絶えず環境の変化を見渡し、自社組織に対してフィードバックをかけることで、リスクビジョンの再構築を進めることである。

次に(4) リスクマネジメントの訓練と実践である。これは平時に訓練を行い、マニュアルの不備を正すとともに、想定外のシナリオがどの時点で発生し、それぞれの担当者のアドリブで対応可能な権限をどの範囲に抑えるかなどを検討する。マニュアルに平時整備しておくべき項目が記されている場合、訓練時に確認し、組織の部門ごとに弱いポイントを強化し、リスクに備える姿勢を伝えることが重要となる。考慮すべき点は、せっかく用意したものが使えない場合が存在することである。平時にそうしたことを含め、訓練し、シミュレーションするなか、どのようにインフラを整備し、具体的にどのように運営をするかなどを細かく取り決めておくことで、実際の事件・事故での対応をスムーズにして、二次災害の拡大を防ぐことが出来る。実践としては、ブログや SNS での情報発信など新しい条件や環境の変化をいかにリスク対策マニュアルの構築に反映していくかは、リスクマネージャーのイメージ能力の深さと広さ、あるいは行動力によって決まる。

これらからリスクリテラシーとはなにかを説明する。リスクリテラシーとは“リスクに接する際、その背景にまで考えを及ぼせ、リスクの波及範囲を正しく見極め、対処する力”である。危険を察知すればするほど、どの状態で危機に対処し、リスクを低減させ、回避すればよいかを判断することが

可能になる。あるいはどちらとも判断できない状況で、次の一手をどう打てばよいかわからなくなる。つまり、リスクリテラシーとは立場に限定されない普遍的なものであり、それぞれの対象者がそれぞれのスタンスに則り、リスクを判断し、行動する力である。図1はリスクリテラシーの概念を図にして、表したものである。研究において、当てはまる部分があり、抜き出しをした。

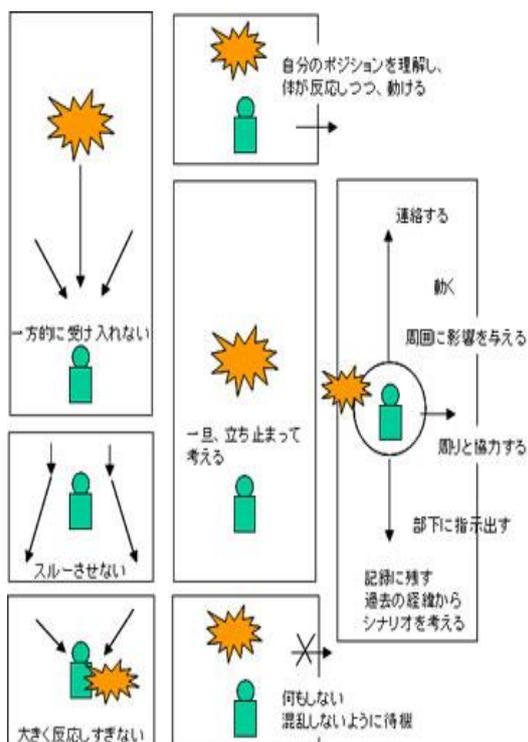


図1 リスクリテラシーの概念 [1]

4. SNS の事例

本節では、SNS 事件の事例を紹介する。その前にインターネットの利用状況やソーシャルメディアの利用状況について説明する。

4.1 SNS 事件概要

インターネットの利用者は、年々、どの年代においても増加傾向にある。それは図2から読み取ることが出来る、全体でも平成22年から26年までで増加し続けている。全体的に横ばいではありながらも、減少することはない。次に図3からこの年代のソーシャルメディアの利用率についてみてみ

ると、十代から三十代までの人が6割を超えていて、どれほどの使用率なのかが見て取れる。これらはスマートフォンの普及により、利用率が増加したと考えられる。スマートフォンによって身近になったネットへの自身の書き込みが若者間で効果的に活用されるようになったためである。

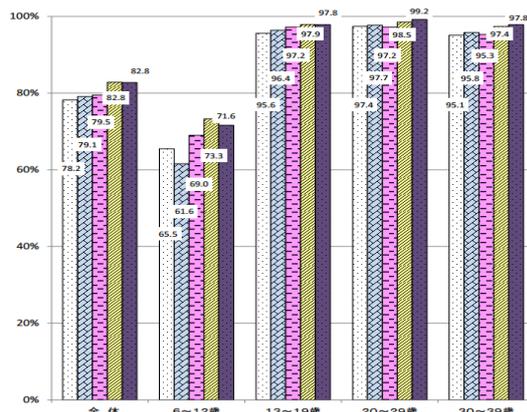


図2 インターネット利用動向(年齢階層別インターネット利用状況) [2]

個人におけるソーシャルメディアの利用状況

13~39歳の利用が6割を、40~49歳の利用が5割をそれぞれ超える。

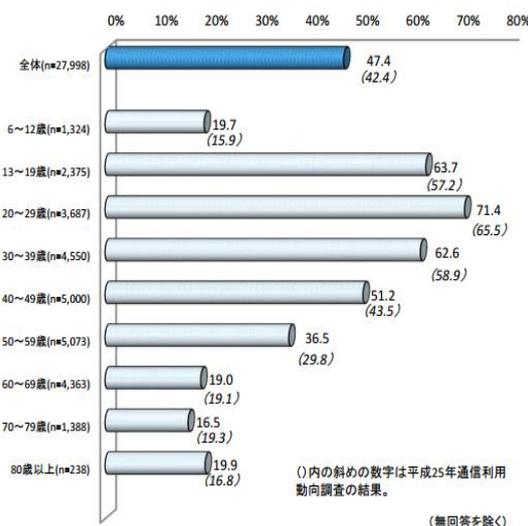


図3 個人におけるソーシャルメディアの利用状況 [3]

次に図4はSNSごとに“炎上”と言葉を入れ、検索した結果の図である。ここから見て分かる通り、2010年から少しずつ検索件数が増加し始める。

本研究で、事例として扱う 2013 年の事件から twitter の検索件数が大幅に増えたということが見て取れる。ここでなぜ twitter のほうだけ伸びて、Facebook では伸びていないかを考えると、twitter が匿名であること、並びに手軽に拡散することが出来、拡散記事を見た人が他人の意見やコメントを見ることもできることが大きく影響する。Facebook は本名制度を採っていたこともあり、自分が使うことに対する危険意識が高いと考えられる。自分が問題を起こした場合、本名である自分自分の仕業だと分かりやすくなるためである。それに対し、twitter は匿名ということで、すぐには自分と結びつかないと考え、公私の区別をうまく意識できていないと考えられる。Twitter は手軽にできる分だけ、意識を軽くしてしまう。



図 4 Google におけるソーシャルメディアの炎上の検索頻度 [3]

そのことを意識して、SNS 事例を調べていくと十代から二十代までのアルバイトの従業員が多くの SNS 炎上事件を起こしていることがわかった。筆者が調べた 30 件のうち 25 件が、その年代によって引き起こされたものだった。その中でなぜ三十代以上では起こることがないのかを考えてみる、ソーシャルメディアの使用率ではさほど事件を起こしやすい二十代と変わらないのになぜなのか、どういった価値観の違いがあるのだろうか。

4.2 SNS 炎上の原因

それは、ソーシャルメディアのリスクと関係があると思われる。ソーシャルメディアのリスクに関する本質は、そもそも SNS 炎上事件の発端である投稿は消しても、投稿内容を消し去ることはできない点にある。投稿自体を消したとしても、拡散された情報自体は複製されてしまっている、現代のネット社会では、こういった複製や保存が容易であるということを忘れてはならない。だからこそ、投稿後の対応策よりも、投稿をしなないための努力が必要となってくる。そして、炎上を助長する要素としてネット上の拡散の速さも存在する。

ソーシャルメディアのリスクに関する本質は、他にも存在する。一つの問題が社会的注目を浴びた時、同じアカウント内やネット上での検索により、過去の投稿が特定できる場合も存在する。自分で何気なく言ったことがまとめられて、個人の情報、身元まで明らかになってしまう可能性もある。

これ自体は自分が気をつけていれば発生しない。しかし、炎上の事例からは、公私の境目が曖昧であるためであるからか、未成年の飲酒や他の炎上事件の要素となりうるものが続々と上がるケースもあった。大学生や高校生の身元や名前なども明らかとなり、その学校に通報されるという事態まで発生した。こうしたネットの危険性を頭では理解していても、実際にはそのことに気付かず、企業と個人の境界が曖昧なままで投稿してしまう場合もある。炎上してから気付く場合が多く、その時にはもう沈静化させることができない。

5. リスクマネジメントの視点からの考察

まずはリスクの原因について述べていく。SNS 炎上と一言で言っても原因が複数存在する。まず一つ目は、“マーケティングコミュニケーションのミス”である。これは公式アカウントからの投稿や情報発信にて不謹慎な投稿が行われる、もしくはその投稿自体の削除、その後問題が起きたにもかか

ならず、横柄な態度を取り、そのことが問題となって発生する炎上である。二つ目は、“顧客サービスのミス”。これは顧客からの発信で、商品やサービスの問題点、不満を投稿されることにより、自社のイメージが低下することである。三つ目は、“一般従業員の不適切な行為・発言”である。これはその会社で働く社員・契約社員、アルバイトからのプライベートな発信で、不適切な発言や情報漏えいが問題となり、炎上するリスクである。

ここで、リスクの原因と影響の大きさの相互関係について考察する。マーケティングコミュニケーションのミスに対しては、企業は自社で発信する情報に対して、責任を感じている状態であると仮定すると、リスクへの意識レベルが高い状態にあると考えられる。意識レベルが高いと、その大きな影響を及ぼすリスクが高いものに対して、問題が発生しないよう対応策を取るため、リスク顕在化の発生頻度は低くなると考えられる。そのため、意識レベルの高さと発生の頻度は反比例する。企業自身が問題を起こしたときは大きく影響を及ぼす。したがって、影響が大きい分、発生頻度が低くなると表すことが出来る。

顧客サービスのミスの影響は、個人での SNS 使用での情報発信のため、それほど大きくない。顧客は個人では故意に企業を貶める投稿をすることは少ないと考えられる。そのため発生頻度も低く、企業に対する影響も小さい。

一般従業員の不適切な行為・発言の影響力は企業の発信ほど大きくはない。しかし、事例などを見ると、リスクへの意識レベルが低いために、リスク顕在化が頻発しやすい。影響力は小さいものと過信し、十分なリスク管理を実施していない場合には同様の事件が起こる。このリスクの特性から、本稿では企業で働く従事者からのプライベートな投稿の炎上を取り出し、分析する。

2014 年の事件数は 640 件近くに上る。そして

2015 年は月ごとの件数は 2014 年を上回っている。

(図 5)

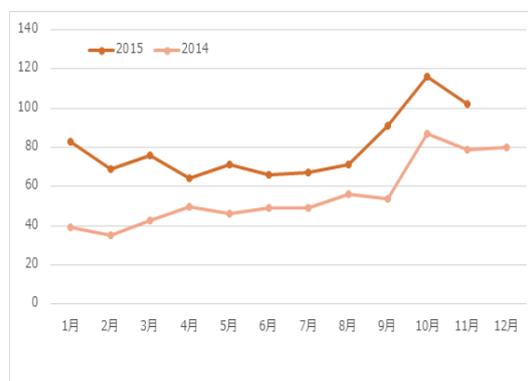


図 5 月間炎上数の推移 [4]

これほど多くの炎上事件がある理由、並びに、それらの割合がどのような職種で発生しているのかを調べるために図 6 を挙げる。図 6 は 2014 年に起きた事件を業界のカテゴリ別に分類した図である。

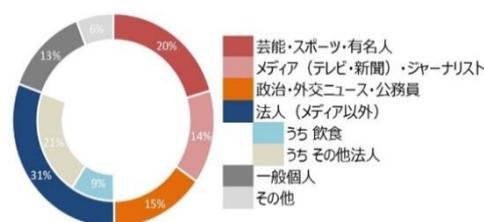


図 6 2014 年度 炎上事例の分類 [5]

これから分かることは、法人が主体となった炎上事例は 228 件あり、その三分之一は飲食業界で発生しているという点である。この分類で筆者が特に注目するのは 2013 年から徐々に増えていき、炎上自体も目にすることが多い法人の飲食である。この年の夏には、2 か月の間で 20 件以上の SNS 炎上事件が発生した。そのため、法人の飲食業界の炎上が一番 SNS 炎上事件で話題に上がりやすい問題であると仮定した。

もうひとつの理由として、SNS を一番身近に感じ

る年代層がアルバイトとして従事していることが挙げられる。2013年の事件の半数以上はアルバイトが原因であった。これらの炎上事件は、炎上から対応、その後、と追いかけてやすすい問題でもあり、一番起こりうる問題である。しかし、その影響力は時に大きなものになってしまう。

6. 提案

企業自体でこういった炎上はないわけではないが、不適切なメッセージを投稿すると、自社への影響が大きい問題へと発展する。そうしない為にも、リスク管理やマニュアル整備がなされ、それによってリスクへの意識が高まり、問題の発生を抑えることができる。これに対して、従業員は企業の情報を持っているにもかかわらず、個人のアカウントによって発信する場合、発言内容がもたらすリスクへの意識が低くなることがある。炎上の事例の中には、友人間でのみ SNS 上でやりとりをしていると思込んでしまい、素早く拡散がされてしまってからその問題について気付く場合が散見される。そこには、リスクが存在するとは考えられておらず、当事者のリスクへの意識レベルは高くないことが伺える。

以上を踏まえて、企業、顧客、従業員の各主体のリスクへの意識、問題発生の頻度、リスクが顕在化した場合の影響との関係を図7に示す。ここで、「企業」とは従業員が企業のアカウントを用いて発信する場合を、「顧客」は顧客が個人のアカウントを用いて発信する場合、「従業員」は従業員が個人のアカウントを用いて発信する場合と定義する。

企業自体の意識のレベルは高いため、炎上事件の発生頻度自体は低い。ただし、その事件がもたらす影響は大きいとみることができる。それに対して、従業員のリスクへの意識レベルは相対的に低い。リスク管理を十分に学んでおらず、SNSの使用においてもプライベートとの区別がついていない

者も少なくない。そのために、事件の発生頻度自体が多くなる。しかし、影響自体は企業が及ぼすものよりは小さなものになると考えられる。ただし、このような事件が多発している現在、影響自体は大きくなってきている。さらに、影響自体は大きくなくても、頻発していることにより関心が高まり易くなってしまいうことも有り得る。

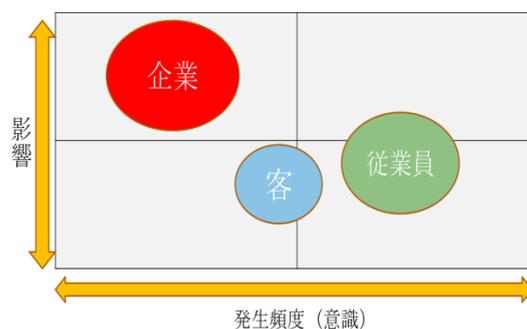


図7 企業と従業員の意識レベルにおける影響の大きさの分布

それは SNS という発信形態によるものではないかと考えられる。SNS において頻発化した炎上事件では、SNS によって拡散する人たちが過敏に反応することが多くなる可能性もある。この場合、従業員の意識レベルはそのままであっても、影響力はさらに大きくなることが予想される。(このことは、図7において、緑色で表される従業員の部分が上部に移動することを意味する。) このことは、企業によって生じる問題の影響力と従業員によって生じる問題の影響力の差が小さくなっていくことを意味する。(図では、赤色で表される企業と緑色で表される従業員がほぼ同じ高さに位置する。) このような状況においては、変化していく SNS に対する対応策を講じる必要がある。具体的には、従業員のリスクへの意識を高めていく必要がある。

顧客の意識とリスク影響の関係については、顧客は SNS をプライベートで使用しているため、意識としてはもちろん企業を貶めようとしているわ

けではない。しかし、企業の落ち度によりその書き込みがされた場合、影響自体は大きくなる場合もある。そのことへの対応策をしっかり実施していくことも、企業の重要なリスク対策の一つである。

従業員の意識レベルを改善するためには、まず、ソーシャルメディアに関する社内ルールを設ける必要がある。それは、従業員がソーシャルメディアを使う際の基本的な姿勢や留意事項をマニュアル化したものである。全従業員に対して、基本方針を定めたマニュアルを作り、そのなかで、従業員の誓約書提出を義務付け、遵守しなかった場合のペナルティと責任を記述する。次に、具体的な Q&A やガイドラインを作ることによって、ソーシャルメディアを使用する際の意識をより具体的にすることができる。これにより、やって良いことと悪いことの区別が付きやすくなる。

同時にソーシャルメディアの特性を理解することも大事になる。投稿は決して自分たちの世界だけ閉じているものではないことを理解する必要がある。ソーシャルメディアを上手に使ってもらなければ、炎上の問題は無くなることはない。投稿に関する予想以上の拡散に対して、横柄な態度を取り、更に拡散を加速させたという例もある。友人間でのみのやり取りだと思いついてしまう事が、問題の発生原因となっている。まずは内と外との区別をしっかりつける教育が必要である。今の時代スマートフォンやパソコンが身近にあり、どんな情報やサイトへもすぐにアクセスし、自分自身からも情報を発信することができる。そんな時代だからこそ、しっかりとした教育を行うべきである。

ここで、ソーシャルメディアに関する社内ルールを設け、具体的な Q&A やガイドラインにより明確なルールを定めることを提案した。その理由は二つある。第一は、事例では損害賠償を請求されるケースもいくつか存在する。損害賠償の金額の事

例から、リスクへの意識を高める対策としての効果が期待される。二つ目は経営者の中には従業員を信頼して誓約書を結ばないところもあると考えられる。事実、筆者のバイト先の経営者からも提出を求められることは無かった。しかし、こうした炎上事件によって倒産など甚大な被害が発生する場合がある。それを予防するためには従業員を信頼するだけでなく、法的な制約が必要になるのではないかと考えられるからである。リスクリテラシーにおいて、図 1 に当てはめて考えると、それぞれの行動に対してワンクッションおいて考えることが大事である。図 1 で表される考えを持つだけで意識が大きく変わってくる。そのためにリスクリテラシーを学ぶことも大事になってくると言える。

7. 結論

SNS の使用に際しては、従業員やアルバイトのリスク管理の意識のレベルが低い場合には、炎上起きやすい状態にある。理由としてはリスクマネジメントやネットのリテラシーの不十分な教育による問題の発生である。意識のレベルを高めるためには、ソーシャルメディアに関する社内ルールを設けることが必要である。さらに、自分自身の明確な判断基準を持つために、具体的な Q&A やガイドラインを作り、明確にルールを定めることで SNS の炎上を低減することも必要である。

これほど SNS の炎上事件が頻発してしまっている理由は、意識レベルが従業員と企業ではかけ離れていってしまった部分があると言える。そのかい離してしまった部分を元に戻せるようにすることも大事である。炎上事件をよく耳にする人は、頻発する事件に対して、過敏に反応するようになってしまうために、事件をより大きな影響力を持っているものと受け取る可能性がある。ソーシャルメディアは、人々が日常使うもので関心をい

い方にも悪い方にも大きく集めてしまう。ソーシャルメディアは「諸刃の剣」となり得ることを理解し、適切な使い方を考えるべきである。

SNS は新しいコミュニケーションのひとつの形であり、コミュニケーションのスピードが格段に速くなり、情報を色々な人へ発信できるようになった。その中でも基本的に炎上事件が起きるのは誰でも見られる投稿が売りの SNS である。新たな友達や色々な人と関わりを持つことができるのと同時に、その関わりあった人たちとも親しく付き合うことができる。しかし、そのように活用できる SNS だからこそ、誰でも自分の発信内容を見ることができる。その内と外の境界が曖昧なまま使用することが問題を引き起こしやすい。SNS によって発生した事件に対しては今までの管理策では扱えないものともなっているのである。

参考・引用文献

1. 林 志行、現代リスクの基礎知識 事例で学ぶ
リスクリテラシー入門、日経 BP 社 BizTech、
2005 年
2. 平成 26 年通信利用動向調査の結果/総務省
/2015.7.17
http://www.soumu.go.jp/menu_news/s-news/01tsushin02_02000083.html
3. インターネットリテラシーの重要性/総務
省/
<http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h26/html/nc143120.html>
4. ネット炎上速報 2015 年総集編を発表
/Eltes/2015.12.24
<https://eltes.co.jp/whatsnew/report2015.html>
5. 2014 年度の”炎上”事例、全 742 件を分類～
増え続ける炎上～/ORM Lab./2015.3.18
<http://www.eltes-orm.com/article/detail.php?b=305>