リスクマネジメント最前線
2012-11

東京海上日動火災保険株式会社
企業営業開発部
〒100-8050
東京都千代田区丸の内 1-2-1
TEL　03-5288-6589
FAX　03-5288-6590
http://www.tokiomarine-nichido.co.jp/
東京海上日動リスクコンサルティング株式会社
http://www.tokiorisk.co.jp/

ソーシャルメディア上のリスクとその対策

近年、ソーシャルメディアの利用者が増加しており、それに伴うトラブルが発生している。ソーシャルメディアとは、参加ユーザー同士が相互にコミュニケーションを取ることができる仕組みを持つインターネット上のサービスで、代表的なものとして、ブログ、mixi・facebook などの SNS（ソーシャル・ネットワーキング・サービス）、YouTube などの動画投稿サイトや 2 ちゃんねるなどのインターネット掲示板、Twitter などが存在する。これらを利用し個人が発信した内容が、インターネット上で瞬く間に拡散し、批判にさらされる（炎上）ケースが増加している。本稿では、従業員などが書き込んだ内容によって企業に影響が出るケースを対象とし、ソーシャルメディア上のリスク傾向とその対策をまとめる。

1. ソーシャルメディアの拡大

平成 23 年の総務省の調査によれば、平成 23 年のインターネット利用者数は推計 9,610 万人と昨年より 148 万人増加した。利用率は 79.1%に上っており、特に 13 歳～49 歳までの世代では、9 割を超えている。スマートフォンやタブレット端末が急速に普及していく中で、インターネットは益々身近になっているといえる。

インターネット利用者が利用する機能・サービスとしては、世代を問わず電子メールの送受信、ホームページ・ブログの閲覧やインターネットショッピングが多いが、特に若い世代の間では、半数近くがソーシャルメディアを利用している状況にある。

2. ソーシャルメディア上での危機事例

ソーシャルメディアの利用が増加する中、軽い気持ちで発信した書き込みが炎上するケースが後を絶たない。利用しているソーシャルメディア上で、個人名や所属企業名等を明らかにしている場合には、その所属先に批判が飛び火し、企業側が対応に追われる事態も発生している。

以下は、2011 年以降に企業等におけるソーシャルメディアを発端とした炎上事例である。

表 1 企業等におけるソーシャルメディアを発端とした炎上事例

業種	媒体	概要	対応	発生時期
サービス業	Twitter	自身が勤めるホテルのレストランに、スポーツ選手と芸能人が来店したことを発言した。また、過去に同様の書き込みを多数していたことも発覚。	ホテルの支配人が謝罪、ホームページ上にお詫びを掲載した。	2011年1月

小売業	Twitter	Twitter で「暴行を受ける女性は自分に責任がある」旨の学生の発言がきっかけで、この学生の個人情報、内定していた企業名が暴露され、企業に対し採用方針や内定決定理由に関する投稿が急増。	同学生の内定は取り消しになったとされている。	2011年2月
小売業	Twitter	スポーツ用品店に来店したスポーツ選手とその夫人を店員が Twitter で中傷。同店員の勤務先まで明らかになり、店員が批判の対象となった。	店員は退職し、所属企業はスポーツ選手と所属クラブに謝罪を行った。	2011年5月
自治体	Twitter	自治体のキャラクターの公式 Twitter が、過去の戦争に関連する発言をし、自治体に対し問い合わせや批判が相次いだ。	公式アカウントは停止され、自治体側が謝罪を行った。	2011年8月
サービス業	Google+	IT 系企業の社員が、採用面接を実況中継し、面接に来た志望者を中傷した。ネット上で批判が相次いだ。	同社は自社サイトにお詫びを掲載した。	2011年8月
製薬業	Twitter	製薬企業社員が、処方薬である睡眠薬を購入し、飲み会で酒に投入して使っていると発言。犯罪行為であるとして批判が相次いだ。	企業から謝罪と弁明のプレスリリースが発表された。	2011年9月
空港	ブログ	管制塔職員が、海外要人のフライトプラン等、業務上の重要機密情報を個人ブログに掲載し問題となった。	守秘義務違反に当たる可能性があるとして、国土交通省が調査を実施した。	2011年9月

出典：各種報道等を基に作成

3. ソーシャルメディア上のリスク特性

炎上事例が頻繁に発生しているにもかかわらず、従業員や役員が依然としてそのリスクを認識できていないケースも多い。ここでは、ソーシャルメディア上のリスクの特徴や傾向をまとめる。

（1） 企業によるコントロールが難しい

個人所有の端末からの発信であれば、イントラネット上の管理とは様相が異なり、企業によるアクセスの遮断や管理が困難である。私用携帯電話での就業時間中のソーシャルメディアへのアクセス禁止については、規制が可能であるが、プライベートな時間でのソーシャルメディアの利用を制限・管理することは、プライバシー保護や表現の自由の観点から見ても、不可能といえる。守秘義務の観点での規制を除けば、企業として全てのリスクをコントロールすることはできない。特にソーシャルメディア上での発言は、“自分が見たことや感じたこと”の個人の感覚での発信になるため、プライベートでの毎日のできごとを綴ることと同じ感覚で、業務に関連する事柄を書き込んでしまうことがある。

また、前述の炎上事例では、アルバイトや内定者など、企業の正社員以外の関係者による書き込みによって企業としての対応を求められるケースも多い。入れ替わりの激しいアルバイトや、内定者に対する会社による規制・管理は特に困難が付きまとうといえる。

（２）　書き込み後炎上に至るまでが短期間である

不用意な発言が書き込まれた後、炎上に至るまでは短期間である。そのため、日々のインターネットの書き込みのモニタリングを実施していない場合、顧客や株主等から指摘を受けるまで、企業側が炎上に気づかないというケースもある。当然のことながら、危機は早く検知すればするほど、被害の極小化が可能であり、定期的なモニタリングで、炎上の火種を掴むことが不可欠といえる。なお、仮に炎上した後に情報を削除したとしても、他のユーザーによってウェブ上の各所に転載されているケースが多い。一旦炎上するとなかなか鎮火しないケースもあるため、迅速かつ適切な対応が不可欠となる。

（３）　企業イメージを毀損する可能性が高い

従業員がソーシャルメディア上で不適切な発信を行うことで炎上し、万一企業名が晒されるような事態になれば、従業員の管理・教育ができていない企業とみなされ、企業イメージを毀損する可能性がある。中でも、炎上した内容が、業務上知り得たものである場合、情報漏えいやプライバシー侵害等として、特に企業が批判を受ける可能性が高い。近年では、こういったネット炎上事例がメディアに取り上げられることも多くなってきており、ひとつの書き込みが企業イメージに与える影響は非常に大きくなっているといえる。

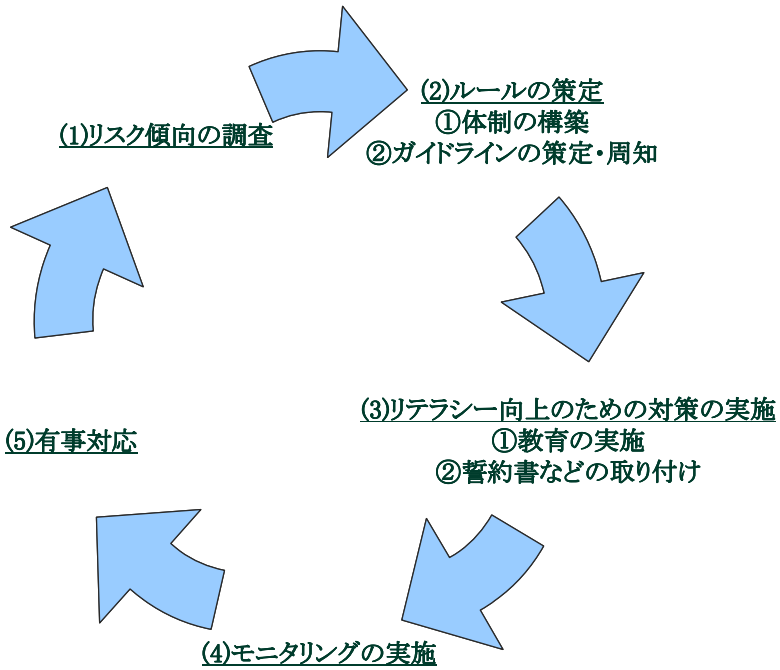
（４）　グローバルなリスクである

ソーシャルメディアは海外でも広く利用されており、日本のみならずグローバルに顕在化しうるリスクである。例えば中国では、“人肉捜索”と呼ばれる、インターネットのユーザーが協力して特定の人の個人情報を暴くという行為が行われている。これまでにも、日系企業の幹部などがこの人肉捜索に晒された事例がある。また、従業員が、企業の労働問題や環境汚染などをインターネット上に告発する事例も存在している。中国においては特に転載が頻繁に行われる特徴があるため、書き込まれた情報は瞬く間に拡散するリスクが高い。新興国においても近年ではインターネットが広く使われるようになってきており、自社の海外拠点での炎上リスクについても、対策を講じておく必要がある。国によっては、内部告発などのインターネット上の書き込みが不買運動につながるケースもある。現地語での書き込みをモニタリングしていくことには技術的な困難も伴うが、対策を講じるべきリスクといえる。

４．ソーシャルメディア上のリスク対策

これまで述べてきたソーシャルメディアのリスク特性を踏まえ、企業としてどのような対策を取るべきかをまとめる。

図１：リスク対策の進め方



（１）　リスク傾向の調査

まず重要なことは、自社にどのようなリスクが存在し、どのようなリスク傾向があるのか分析を行うことである。これまでにトラブルになりそうな書き込みはなかったのか等、ソーシャルメディア上のリスクの洗い出しを行う。

それらを分析すると、例えば労働環境に不満を持っている従業員の内部書き込みが多かったり、仕事で経験したことを綴った書き込みが多いなど、自社の特徴が見えてくる。その特徴を踏まえ、対策を講じていくことが望ましい。

（２）　ルールの策定

①　体制の構築

リスク傾向を掴んだら、平時のリスク対策・有事対応のための体制を構築する。担当となる部署、モニタリングを行う担当者、意思決定者、そしてソーシャルメディアを利用している従業員からの相談窓口など、担当を予め決定する。これら体制や有事対応については、有事の際にも迅速な対応が可能となるよう、マニュアル化しておくことが求められる。

【ソーシャルメディア対応のマニュアル構成例】

第1章　総則
- Ⅰ. 目的
- Ⅱ. 用語の定義
- Ⅲ. 従業員の責務
- Ⅳ. マニュアルの維持管理

第2章　平時の対策
- Ⅰ. 主管部署
- Ⅱ. 平時の体制
- Ⅲ. モニタリングの実施
- Ⅳ. 教育・訓練の実施

第3章　リスクカテゴリ別 危機レベル設定
- Ⅰ. 危機モード
- Ⅱ. 警戒モード
- Ⅲ. 注意モード

第4章　危機検知時の対策
- Ⅰ. 検知時の連絡体制
- Ⅱ. 危機別対応部署一覧
- Ⅲ. 危機レベル分けの実施

第5章　危機モード下の対策
- Ⅰ. 対策本部の設置・その実施事項
- Ⅱ. 広報対応を実施する場合
- Ⅲ. 削除申請を実施する場合
- Ⅳ. 法的手段を講じる場合

第6章　警戒モード下の対策
- Ⅰ. 対策本部事務局の設置・その実施事項
- Ⅱ. 広報対応を実施する場合
- Ⅲ. 社内に是正指示を出す場合

第7章　注意モード下の対策
- Ⅰ. 主管部署の実施事項
- Ⅱ. 広報対応を実施する場合
- Ⅲ. モニタリングを強化する場合

＜巻末資料＞
- Ⅰモニタリングサイト一覧
- Ⅱメディア関係先一覧
- Ⅲリリース文案

② ガイドラインの策定・周知

多くの企業で策定が進んでいるコンプライアンス関連規定や情報セキュリティ規定などについても、ソーシャルメディアにおけるリスクも踏まえた対応を講じておくことが重要である。また、ソーシャルメディア利用上のガイドラインを定め、不適切な書き込みが自社と本人に対しどのような結果・損害をもたらすのかを踏まえ、利用上のルールをアルバイト等を含む従業員に対し周知徹底することが望ましい。

【ソーシャルメディア利用に当たって個人が留意すべき事項の一例】

以下の内容は書き込みをしない

- **業務上知り得た機密情報**
  - 自社に関する未公開情報
  - 自社の製品・サービスに関するノウハウ、機密情報
- **個人情報（プライバシーの侵害に当たる内容）**
  - 顧客・取引先企業、同僚・上司などの名前、性別、年齢、居住地など
- **著作権や商標権を侵害する書き込み**
  - 他人の作品や他社の商標などを勝手に利用した書き込み
- **名誉毀損にあたる書き込み**
  - 個人や企業等への誹謗中傷
  - 事実無根の情報により他人を批判するような書き込み
- **内容によっては他人の感情を害する恐れのある書き込み**
  - 思想、政治、信条、宗教、人種、民族、身体・精神障害、犯罪歴、事故情報、保健医療等、機微な内容
  - 読んだ相手が精神的、経済的、社会的に不利益や差別を受ける可能性のある内容
- **なりすましとみなされる書き込み**
  - 自社、自社の製品・サービスを絶賛するような書き込み
- **犯罪行為をしたと思われる内容の書き込み**
  - 飲酒運転など違法行為を行ったと受け取られる書き込み

（３） リテラシー向上のための対策の実施

① 教育の実施

ソーシャルメディアの炎上を防ぐためには、従業員一人ひとりのリテラシーの向上が何よりも重要となる。そのためには教育の実施が求められる。教育では、ソーシャルメディアに潜むリスクの特徴などを、実際の炎上事例を踏まえながら紹介し、従業員のリスク感性を磨いていく。教育の場では、“書き込んではいけないこと”の説明が重要である。自社のガイドラインを踏まえながら、業務上知りえた内容の書き込みを禁止すると共に、社会的に批判を浴びるような発言についても控えさせる必要がある。加えて、各ソーシャルメディアの特徴や、利用する場合に留意しておくべきポイントなどについても紹介しておくと良い。書き込みの内容によっては、先に策定したルールに基づいて懲戒処分等を受ける可能性についても言及しておく。

② 誓約書などの取り付け

教育の実施に加え、業務上知り得た事柄をソーシャルメディア等に書き込まない旨の誓約書を取り付けることも一案である。拘束力は期待できないが、“ソーシャルメディア等の利用時には注意しなければならない”という意識を醸成することで、一定の効果は期待できるものと考えられる。

（４） モニタリングの実施

前述の通り、ウェブ上の炎上は瞬く間に広がる。いち早く炎上を検知するためには、モニタリングを定期的に実施することが重要である。ただし、多岐にわたるソーシャルメディアで日々投稿される膨大な量の書き込みを人手でチェックしていくことは不可能に近い。昨今では、ウェブ上の書き込みを効率的にモニタリングできるサービスも提供されているため、それらを活用し、効率的に自社に関連する書き込みをチェックしていくことが求められる。できる限り迅速にリスクを検知して対処することで、大規模な炎上を防ぐことが可能となる。

モニタリングを行う場合には、企業名や商品・サービス名、役員の名前など、書き込まれる可能性のあるキーワードを選定することが重要である。企業名などに関し、インターネットユーザーのみが使う特定の呼び名などがあれば、それも併せてモニタリングする必要がある。

（５） 有事対応

万一、炎上した場合には、まず炎上した原因を分析し、企業として正式に謝罪をすべきか否か、また発端となった従業員等への対応について、意思決定する必要がある。謝罪をする場合には、ホームページ上にお詫びを掲載するのか、記者会見を実施するのか、その事例がどの程度社会に影響を及ぼしたかによって、最も適した手法を選択すべきである。また、謝罪文の内容が不適当だとして更なる炎上につながったケースもあるため、内容を十分精査する必要がある。なお、炎上しているソーシャルメディア上で反論をする等の行為は、火に油を注ぐ結果になりうるため、絶対に行ってはならない。

５．最後に

誰でも自由に意見を発信できるようになった現在、ソーシャルメディアの炎上リスクは、どの企業にも発生しうる身近なリスクとして認識し、対策を強化していく必要があるといえよう。発信する本人は悪意なく行動していたとしても、それが炎上した場合、企業に与える影響は計り知れない。過去の炎上事例を参考とし、アルバイト等を含めた従業員のリテラシーを高めつつ、有事にも備えられる体制を構築することが望まれる。

（2012 年 8 月 1 日発行）