

経営インパクトをもたらすフェイクニュースと企業の対策

ビジネスリスク本部 主任研究員 土井慎一（専門分野：コーポレートガバナンス・リスクマネジメント・危機管理）

要約

近年、SNS 等における事実と異なる情報、いわゆる「**フェイクニュース**」の拡散は、**企業の信用低下や売上減少、株価下落等をもたらす重大な経営リスク**となっている。日本国内のフェイクニュースに関する各種対策は、総務省研究会等¹において政策的な議論がなされている一方で、企業活動におけるフェイクニュース対策の在り方については、これに特化したガイドラインやフレームワークは存在せず、対策は各企業の裁量に委ねられている。

本稿では、広くコンセンサスを得ている情報の類型パターンを基にフェイクニュースの様態を明らかにした上で、企業がフェイクニュースに対して取るべき基本的な対応方針を9パターンに整理する。さらに、ISO/IEC 27035 情報セキュリティインシデントマネジメントを参考に、5段階からなる企業のフェイクニュース対策の全体像を提示する。

目次

1. フェイクニュースの様態	2
(1) 偽情報・誤情報の7類型	2
(2) 8つの動機のパターン	3
2. 企業がとるべき基本的な対応方針	3
3. 企業におけるフェイクニュース対策の在り方	5
(1) 体制整備	5
(2) モニタリング	6
(3) 基本方針の決定	6
(4) 影響度評価・対応実施	6
(5) 検証・改善	7
4. おわりに	8

1. フェイクニュースの様態

近年、SNS 等における事実と異なる情報、いわゆる「**フェイクニュース**」の拡散は、**企業の信用低下や売上減少、株価下落等をもたらす重大な経営リスク**となっている。フェイクニュースとは、一般には偽情報（disinformation）や誤情報（misinformation）に基づく SNS 等ソーシャルメディア上における各種コンテンツを指し、それらは必ずしもニュースの体裁を取っておらず、個人による私的発信から国家による情報操作に至るまで幅広い様相を呈している。フェイクニュースの様態を理解する上では、クレア・ウォードル（Claire Wardle）氏²の提唱する「偽情報・誤情報の 7 類型」と、その解説で用いられる 8 つの動機パターンによる整理が有用である。

(1) 偽情報・誤情報の 7 類型

偽情報・誤情報は、その欺く意図の大小に応じて、図表 1 の通り 7 つの類型に大別される。

■ 図表 1：偽情報・誤情報の 7 類型

欺く意図	分類	概要
小 ↓ 大	① 風刺またはパロディ Satire or Parody	悪意はないが、人を騙す可能性のあるコンテンツ。
	② 誤った関連性 False Connection	見出しやタイトルが内容と一致していないコンテンツ。
	③ 誤解を招くコンテンツ Misleading Content	ある情報について、誤解を招くように利用すること。
	④ 誤った文脈 False Context	真の情報が、誤った文脈とともに共有されること。
	⑤ 詐欺的コンテンツ Imposter Content	情報源を特定の正規組織や人物等に偽装・なりすましている情報。
	⑥ 改ざんされたコンテンツ Manipulated Content	本物の情報や画像が、一部改ざんされている場合。
	⑦ 捏造されたコンテンツ Fabricated Content	100%虚偽であり、人々を欺くことを目的に新たに生成されたコンテンツ。

出典：Wardle, C. (2017) “Fake news. It’s complicated.” First Draft を基に筆者作成

これらの内、例えば「⑦捏造されたコンテンツ（Fabricated Content）」に係る企業の実例としては、金融機関で取り付け騒ぎが起こる旨の 100%虚偽の投稿が SNS で拡散されたケースが該当する。このケースではステークホルダーに大きな混乱が生じ、当該金融機関は公式 HP や会見を通じて、投稿が虚偽であることを繰り返し説明し、結果的に投稿者は逮捕された。このほか、「②誤った関連性（False Connection）」の実例として、自社商品名のタイトルとともに全く異なる他社商品の写真が SNS に投稿されたケースや、「⑤詐欺的コンテンツ（Imposter Content）」の実例としては、公式を装ったなりすましアカウントによる SNS 投稿が該当する。

(2) 8つの動機のパターン

上記7種類の偽情報・誤情報について、ウードル氏は図表2の通り、8つの動機のパターンも提示している。

■ 図表2：8つの動機のパターン

分類	概要
(ア) 粗末なジャーナリズム Poor Journalism	取材不足や勘違いによる誤報あるいは不正確な報道
(イ) パロディ Parody	うけねらいや娯楽目的
(ウ) 挑発または嫌がらせ To Provoke or 'Punk'	個人や集団への攻撃や嫌がらせ目的
(エ) 熱意 Passion	信念に基づく発信・拡散
(オ) 党派心 Partisanship	特定の党派や派閥を有利にする目的
(カ) 経済的利益 Profit	広告収益等の金銭的利益目的
(キ) 政治的影響力 Political Influence	世論誘導や選挙影響を狙う政治目的
(ク) プロパガンダ Propaganda	特定の理念や信条を広めるイデオロギー目的

出典：Wardle, C. (2017) "Fake news It's complicated." First Draft を基に筆者作成

例えば、先述した金融機関における図表1「⑦捏造されたコンテンツ」のケースは「(ウ) 挑発または嫌がらせ (To Provoke or 'Punk')」あるいは「(エ) 熱意 (Passion)」といった動機に根差していたほか、図表1「②誤った関連性」に係る投稿は「(ア) 粗末なジャーナリズム (Poor Journalism)」、すなわち勘違いに根差している可能性が高い。また、公式のなりすましによる図表1「⑤詐欺的コンテンツ」は、例えば、なりすましアカウントからの SNS 投稿による海賊品の販売サイトへの誘導を目的とした「(カ) 経済的利益 (Profit)」に根差しているものであろう。

もちろん、ある偽情報・誤情報について複数の動機が混在することもあり得るほか、SNS 等での発信当初は単なる「(イ) パロディ (Parody)」目的だったものが、インプレッションを稼ぐための金銭的な「(カ) 経済的利益」目的に変わるなど、偽情報・誤情報の動機が拡散される過程で変質していく場合もある。

以上のように、企業の直面するフェイクニュースの様態は、(1) 偽情報・誤情報の7類型及び(2) 8つの動機のパターンを組み合わせることで、一定の説明が可能である。

2. 企業がとるべき基本的な対応方針

企業が影響をうけるフェイクニュースに対して取るべき基本的な対応は、先述したフェイクニュースを構成する2つの要素の組合せにより大きく左右される。例えば偽情報・誤情報の類型が同じ「捏造されたコンテンツ」の場合でも、その動機が「挑発または嫌がらせ」であれば、企業はニュースバリューを高めないために、繰り返しの否定発信を避けた方がよい場合がある。他方で、動機が「経済的利益」である場合は、企業は損失を回避し、ステークホルダーへの注意喚起を促す観点から、毅然とした対応で繰り返し否定する必要があり、望ましい対応は全く異なるものとなる。

そこで、国内外の複数の企業事例に関して、先に述べた偽情報・誤情報の7類型と動機の8種の組合せに照らし、企業がとるべき基本的な対応方針を検討すると、図表3のとおり整理できる。理論上は7類型×8動機の56

パターンであるが、類似する対応が導かれる類型・動機は統合し、本稿では 3 類型×3 動機の 9 パターンに整理した。なお、整理に当たり動機を「企業への加害性の大小」を尺度として並べ替えている。

■ 図表 3：偽情報の性質をふまえて企業がとるべき基本的な対応方針（9 パターン）

類型 動機		（欺く意図）		
		小	中	大
		①風刺またはパロディ	②誤った関連性 ③誤解を招くコンテンツ ④誤った文脈	⑤詐欺的コンテンツ ⑥改ざんされたコンテンツ ⑦捏造されたコンテンツ
小 （企業への加害性）	(ア)粗末なジャーナリズム (イ)パロディ	・ノーリアクション ・安易な全面否定の回避	・事実の全体像を文脈・時系列と合せて提示	・事実関係を迅速に提示し否定
	(ウ)挑発または嫌がらせ (エ)熱意 (オ)党派心 (キ)政治的影響力 (ク)プロパガンダ	・誤解を招いている旨告知 ・投稿者との対立姿勢の回避	・政治的・思想的中立性を維持 ・事実の全体像を文脈・時系列と合せて提示	・ファクトチェック結果と共に事実関係を示し否定 ・否定発信の過度な繰り返しの回避
	大 (カ)経済的利益	・経済的損失を看過せず警告	・顧客等ステークホルダーへ事実関係を周知 ・商標権等に基づく法的措置を辞さない対応	・事実の全体像を迅速に提示し否定 ・あらゆる法的措置を辞さない毅然とした対応 ・不用意な低姿勢の回避

出典：Wardle, C. (2017) “Fake news It’s complicated.” First Draft を基に筆者作成

上記 9 パターンを概観すると、**欺く意図（横軸）が大きくなるにつれ、企業は事実関係を迅速に提示し、明確に否定する対応が求められる。**特に「⑤詐欺的コンテンツ」等の欺く意図が大きい類型では、ノーコメントでの放置を避け、確実な否定発信を行う必要がある。一方、欺く意図が小さい類型では、投稿者との不要な摩擦を避ける意味で、ノーリアクションや告知に留めるなど、比較的穏健な対応が想定される。また、**企業への加害性（縦軸）が高まるほど、単なる事実提示に留まらず、警告やステークホルダーへの周知等、積極的な対応が必要となる。**特に「（カ）経済的利益」を動機とするケースは、実害の拡大を防ぐためにも毅然とした対応が求められる。このように、両軸の組合せに応じて、企業が取るべき基本的な対応方針は全く異なっている。

例えば上記の内、「⑦捏造されたコンテンツ」×「（ウ）挑発または嫌がらせ」の組合せに係る対応の好事例として、コロナ禍における米国製薬企業に関する実例が挙げられる。このケースでは、「製薬企業 CEO が、ワクチンに関する詐欺罪により FBI に逮捕された」旨の偽トピックがインターネット上に投稿されたところ、当該トピックが本物のロゴを使用したニュースを装っていたため、SNS 上で爆発的に拡散され、同社の信頼性を揺るがす炎上にまで発展した。これに対し、同社は特に偽情報を否定する公式声明を发出せず、CEO 自身が即日生放送のテレビ番組に出演することで「逮捕されていない事実」を体現し、およそ 1 週間前後で主要メディアにおける炎上は沈静化した。

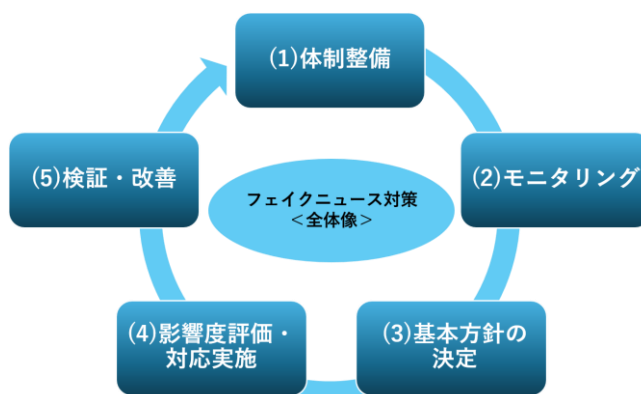
本事例を図表 3 に照らすと、否定発信の過度な繰り返しの避けつつ、事実関係を提示することで、レピュテーションの低下や危機対応コストの増大を回避した事例であったと言えるだろう。本事例等も踏まえ、**企業がフェイクニュースに対応する際には、致命的な被害を避けるためにも、図表 3 で述べた基本的な対応方針を選択・決定し、自社内で意思統一を図る必要がある。**

3. 企業におけるフェイクニュース対策の在り方

日本国内のフェイクニュースに関する各種対策は、総務省研究会等において政策的な議論がなされており、近年では「情報流通プラットフォーム対処法（2025 年 4 月施行）」により、大規模プラットフォーム事業者における投稿削除の迅速化等が義務付けられた。他方で、企業活動におけるフェイクニュース対策の在り方については、これに特化したガイドラインやフレームワークは存在せず、対策は各企業の裁量に委ねられている。

そこで、前項で述べた基本的な対応方針の選択・決定と対応実施のプロセスも含め、企業におけるフェイクニュース対策の全体像を ISO/IEC 27035 情報セキュリティインシデントマネジメント³を参考に検討すると、以下の 5 つのフェーズを繰り返して改善を重ねていくことが望まれる（図表 4）。

■ 図表 4：フェイクニュース対策の全体像



出典：ISO/IEC 27035 を参考に筆者作成

※ ISO 規格は基本的に自社影響下にある情報システムについて対応する一方で、フェイクニュース対策は後述のとおり、常に変化する自社外部環境を分析しながら対応を講じる点で大きく異なる。

企業におけるフェイクニュース対策としては、（１）体制整備：平時の準備を整え、（２）モニタリング：異常な情報の拡散を検知し、（３）基本方針の決定：事実確認の上、基本的な対応方針を決定し、（４）影響度評価・対応実施：拡散状況等に応じた具体的な対応を実施、（５）検証・改善：振り返りを行う、といった流れが想定される。各フェーズのより具体的な取組内容は、以下のとおりである。

（１）体制整備

「体制整備」は後述する（２）～（５）の対応に備えて、予め自社の体制を整備するフェーズであり、ここでは組織体制、プロセス及び文書・ツールを定めるとともに、それらの土台となる全社的な意識醸成を図るフェーズである。

まず**組織体制**としては、有事の際にイニシアチブを取って対応を行う部署（リスクマネジメント部門等）を定めるとともに、後述する SNS 等の日常的なモニタリング活動を行う部署（広報部門等）を定め、有事の際は必要に応じて対策本部を立ち上げるなど、両者が迅速な連携のもと対応することを取り決める。

また**プロセス**としては、対策の全体像として述べた各プロセスを経ることを社内において取り決めるとともに、対策の妥当性検証として定期的な訓練実施等を定める。

さらに**文書・ツール**として、組織体制及びプロセスで取り決めた内容を危機管理規程等の形で文書化するとともに、後述する（２）モニタリングから（３）基本方針の決定に移行する際の基準となるモニタリング指標及び閾値を設定するほか、（４）影響度評価・対応実施において必要となる自社への影響度及び情報の拡散トレンドを図るための指標及び閾値を設定するなど、実際の対応で必要となる各種ツールの検討・作成を行う。

その上で、**全社的な意識醸成**として、文書・ツール等により定めた組織体制及びプロセスを、リスク管理委員会における議題として取り上げつつ、社内研修等により周知し、有事の際の全社対応が可能な状態としておく。

(2) モニタリング

平時において、SNS 等の自社や自社サービスに係る投稿を監視し、異常な拡散がないか検証するフェーズである。

具体的には、広報部門による生成 AI を活用したソーシャルリスニング等により、一定期間内の自社関連ワードの SNS 投稿上昇率やニュースサイトにおけるトレンド等を**モニタリング指標として監視し、必要に応じて結果をリスク管理委員会等で社内共有**する。一連の活動において、各指標で定める閾値を上回るなど**異常な情報拡散が認められた場合、広報部門からリスクマネジメント部門に速やかに情報共有**し、(3) 基本方針の決定へ移行する。

(3) 基本方針の決定

(2) モニタリングで異常な拡散が確認された場合に、当該拡散情報がフェイクニュースであるかを評価し、基本的な対応方針を決定するフェーズである。

具体的には、広報部門とリスクマネジメント部門とで協力し、まずは自社が直面している**拡散情報に関する事実確認（ファクトチェック）**を行う。その上で、拡散情報がフェイクニュースであった場合、情報の 3 類型×3 動機を検証した上で、その組合せに応じた**基本的な対応方針を決定・社内共有**し(4) 影響度評価・対応実施へ移行する。

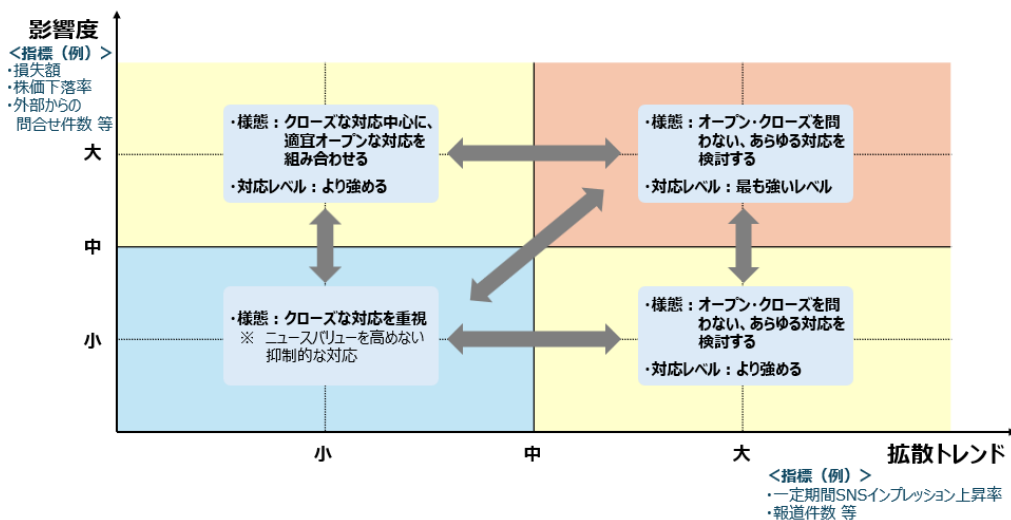
なお、自社でも真偽不明の情報については、事実関係を明らかにしなければ適切な対応方針を検討できないため、必要に応じて第三者機関の協力を得るなど、慎重なファクトチェックを要する。

(4) 影響度評価・対応実施

(3) において決定した基本的な対応方針に従いつつ、フェイクニュースの「影響度」及び「拡散トレンド」に応じた個別の対応を実施するフェーズである。

具体的には、リスクマネジメント部門は、各部門による損失額等「影響度」の情報と、広報部門によるリアルタイムの「拡散トレンド」の情報提供を受け、それぞれを縦軸・横軸に配置した**対象となるフェイクニュースの現状と個別の対応を判断するマトリクス（図表 5）にプロットし、自社が現在位置している象限を把握**する。その上で、予め**個別の対応を整理した資料（図表 6）等を基に、自社の位置する象限に適した対応を検討・実施**する。

■ 図表 5：対象となるフェイクニュースの現状と個別の対応を判断するマトリクス



出典：筆者作成

※ 影響度（縦軸）・拡散トレンド（横軸）として設定する指標・閾値（小・中・大の値）は、(1) 体制整備において定める。

■ 図表 6：個別の対応方法の一覧（例）

様態	対応レベル	個別の対応方法（例）
クローズ （水面下）	弱 ↓ 強	不用意な発信等行わないよう社内向け注意喚起
		コールセンター・営業等の対応方針を統一
		法的措置に備え、外部専門家へ相談・検討
		プラットフォーム事業者への投稿削除依頼
オープン	弱 ↓ 強	公式 SNS でのウィットを交えた発信
		公式 SNS での対話チャネルの公開
		公式 HP での事実関係のプレスリリース
		公式 HP での法的措置を辞さない旨の警告
		メディアへの積極的な情報提供
		経営層等による会見による正しい情報の説明

出典：筆者作成

※ 有事の際に個別の対応の選択に漏れないよう、（１）体制整備において検討し定める。

なお、図表 6 等を基に個別の対応を実行する際には、**（３）において決定した基本的な対応方針を順守することに留意**する必要がある。先に述べたように、情報の動機のパターンによっては、繰り返しオープンな否定発信を行うことでかえって事態を悪化させる可能性もあることから、対応を実行する際は、改めて（３）で決定した基本的な対応方針を逸脱していないか確認を行う。

例えば、自社が上記マトリクスにおいて影響度・拡散トレンドともに高い右上の象限に位置し、最も強い対応レベルを要する場合にも、投稿の動機が「熱意」や「党派心」等の感情的なものである場合は、基本的な対応方針としての「否定発信を過度に繰り返さない」ことを踏まえ、プレスリリースや会見等のオープンかつ強いレベルでの個別の対応は必要最小限とし、プラットフォームへの投稿削除依頼等のクローズかつ強い対応を重視する。他方で、自社がマトリクスの右上の象限に位置し、かつ投稿の動機が「経済的利益」の場合は、基本的な対応方針としての「あらゆる法的措置を辞さない」「不用意な低姿勢を避ける」といったことを踏まえ、オープン・クローズを問わず、あらゆる強いレベルの対応により対抗する。このほか、影響度・拡散トレンドともに低いマトリクスの左下象限にあっては、ニュースバリューを高めないためにも一度静観するか、個別の対応を取る場合にもクローズな対応を重視すべきである。

なお、リスクマネジメント部門は、フェイクニュースが拡散する過程でその動機が変化していないか、派生的な偽情報・誤情報が生じていないか注意し、状況の変化が著しければ、基本的な対応方針の見直しを検討する。

（５）検証・改善

フェイクニュースの拡散トレンドが収束して一定期間が経過した後、一連のフェイクニュース対応を振り返り、（１）体制整備に還元するフェーズである。

具体的には、対応にあたった社員の意見を集約し、組織間連携においてボトルネックとなったことや、予め定めたプロセスにおいて不足していた観点、各指標や閾値の見直すべき点等を抽出する。また、対応実施によるマスメディアや SNS 等の外部の反応について情報を収集し、必要に応じてリスク管理委員会等に諮りつつ、体制の見直しを行う。なお、対外的な事後対応として、株主や取引先等ステークホルダーへの説明のため、対応に要した期間や被害額を整理する必要があるほか、被害の様態によっては発信者等との法的争訟にも対応する必要がある。

4. おわりに

近年、生成 AI の加速度的な進化に伴い、真の情報と見分けのつかないディープフェイクが拡散される事例も頻発しており、企業を取り巻く外部環境は今後さらに複雑さを増していくものと予想される。

企業においては、今後はフェイクニュースと共存する前提のもと、自社がフェイクニュースによって受ける影響を最小化する取組を推進するとともに、組織全体としてのレジリエンスを一層高めていく必要がある。

そのためには、適切なリスク評価やリスク対応計画の策定等、日ごろのリスクマネジメントを確実に実施するとともに、有事に備えた組織体制やプロセス、文書・ツールを定め、定期的な訓練等を通じた見直しを含む危機管理体制の一層の強化が不可欠である。

[2026 年 10 月 9 日発行]

¹ 総務省研究会等

・デジタル空間における情報流通の健全性確保の在り方に関する検討会

https://www.soumu.go.jp/main_sosiki/kenkyu/digital_space/index.html

・デジタル空間における情報流通の諸課題への対処に関する検討会

https://www.soumu.go.jp/main_sosiki/kenkyu/digital_shokadai/index.html

² Wardle, C. (2017) “Fake news. It’s complicated.” First Draft

<https://firstdraftnews.org/articles/fake-news-complicated/>

³ ISO/IEC 27035 Information technology — Information security incident management

当該規格では、情報セキュリティインシデントマネジメントを 5 つのフェーズ（計画及び準備、検知及び報告、評価及び決定、対応、学んだ教訓）に分けて整理している。



東京海上ディーアル株式会社

ビジネスリスク本部 土井慎一 主任研究員（専門分野：コーポレートガバナンス・リスクマネジメント・危機管理）
〒100-0004 東京都千代田区大手町 1-5-1 大手町ファーストスクエア ウエストタワー23F
Tel. 03-5288-6580 Fax. 03-5288-6590 <https://www.tokio-dr.jp/>