新たな AI 領域における企業のリスクとレピュテーション

著者： Rhett Skelton, Michael McMenemy, Jonathan Newton

GAME CHANGERS

Ipsos

KEY TAKEAWAYS:

1. **企業のレピューテーションとビジネスに対する新たな脅威:** AI は、レピュテーションを守ろうとする企業に独特の脅威をもたらします。世界中の悪意のある者が、個人的な利益のためにソーシャル エンジニアリング、画像やビデオの捏造、フィッシング/詐欺の分野で AI の機能を利用し、その過程で企業のレピュテーションに重大な損害を与える可能性があります。

2. **自分自身を知る:** これらの脅威の潜在的な影響を理解するには、企業のレピュテーションが現在どのような位置にあるのか、主要なステークホルダーが何を期待しているのかを知る必要があります。

3. **相手と同じ手段を用いる:** 絶え間なく変化するレピュテーションの環境において、企業が脅威に先んじるためには多面的な AI 主導の戦略を採用することが現在不可欠です。従来のリサーチソリューションとデジタル監視を組み合わせることで、既知と未知の両方の脅威からレピュテーションを確実に保護します。

4. **将来の計画:** AI、データ サイエンス、サイバーセキュリティ、ポリシー、コミュニケーションの専門家で構成される社内タスクフォースが、企業のレピュテーションを守る中心となります。組織全体の AI リテラシーを向上させ、AI による潜在的なリスクを特定することで、AI を利用した脅威に迅速に対応できるようになります。

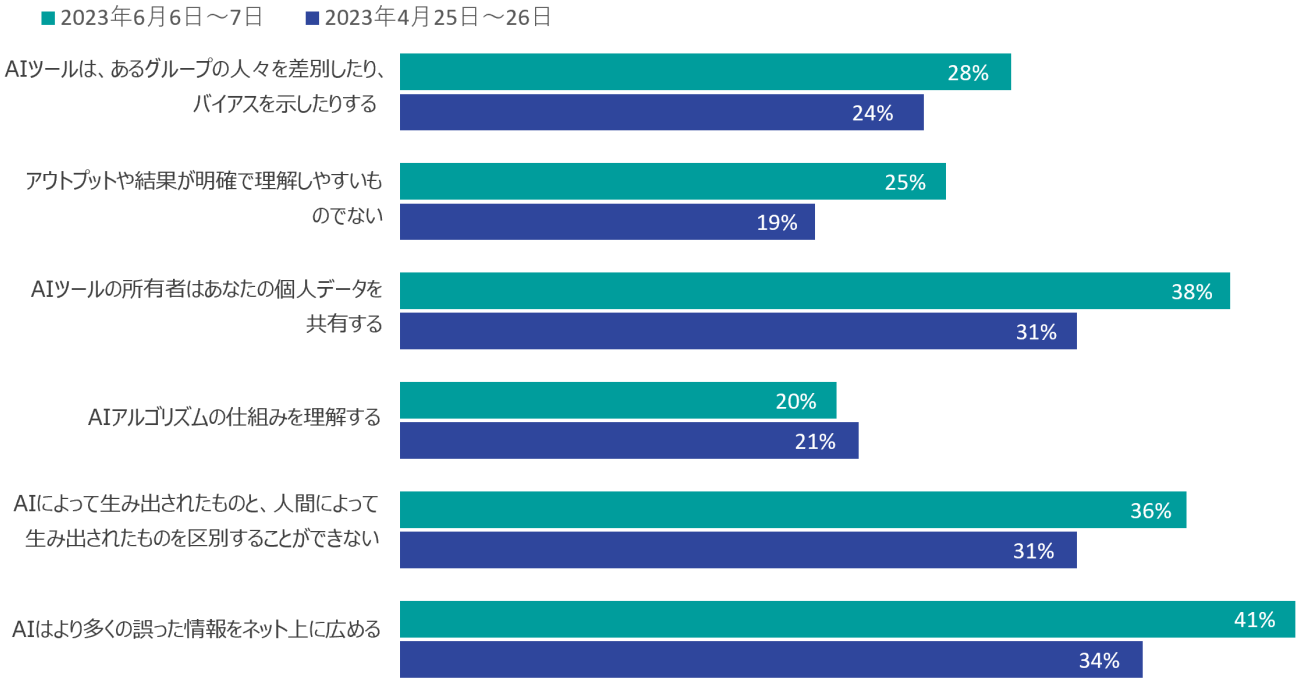
「あなたのアイデンティティはあなたの影のようなものです。常に目に見えるわけではありませんが、常に存在します。」– スタニスワフ・レム、ソラリス

人工知能（AI）は、産業を形成し、ビジネスを変革し、私たちの生活のあらゆる側面に影響を与える強力な力として出現しました。その普及と民主化は前例のない急速な進歩をもたらし、効率を向上させ、カスタマーエクスペリエンスを向上させる革新的なアプリケーションへの道を切り開くでしょう。

同時に、Ipsos Consumer Tracker の最近の調査によると、AI への不安も高まっています。AI 特有の課題と、AI がレピュテーションやブランドを守ろうとする大企業にもたらす前例のないリスクは、あまり世間で注目されていません。

AI に対する懸念の度合いは高まっている

AI の可能な用途について考えるとき、次のそれぞれについて、どれくらい心配していますか? – とても心配しているの割合



Base : 1,108 名(アメリカの成人)、2023 年 6 月 6 日から7日にかけて実施
Source: Ipsos Consumer Tracker

AIの理解はまだ遅れている

AIの理解 **当てはまるの割合（31カ国平均）**

Base：22,816 人（31 か国の 75 歳未満の成人）、2023 年 5 月 26 日から 6 月 9 日にかけて実施 -- インドを除くすべての国でオンラインのみ。
「世界の国平均」は、調査が実施されたすべての国の平均結果を反映しています（人口に合わせて調整されていません）。
Source：イプソス | AI 2023 に関する世界的な見解

たとえば、AI テクノロジーの一つである生成AI は、 シンセティック・メディア（合成メディア）の作成を可能にし、特にクリエイティブ産業にプラスの貢献をもたらす計り知れない可能性をもたらします。同時に、シンセティック・メディアはあらゆるビジネスに重大なリスクをもたらします。テクノロジーにあまり詳しくない詐欺師であっても、AI の助けを借りて、誰でも、洗練されたスキームでリアルな偽のオーディオおよびビデオ コンテンツを作成できるようになりました。悪意のある者は、生成 AI をさらに悪用して、詐欺やフィッシングの試みに使用される不正コンテンツを作成したり、企業のレピュテーションを傷つけたりする可能性もあります。

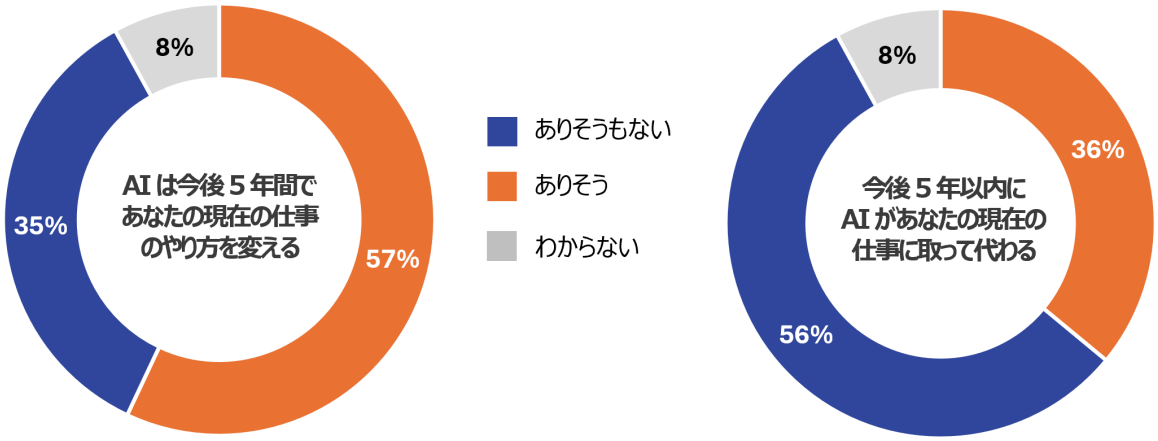
この新しい AI の時代に、企業は新たなリスクにどのように対処し、自社のブランドを守るのでしょうか?主な手順は次のとおりです。

1. AI の普及による危険性、または悪意のある者がテクノロジーを使用する可能性のあるさまざまな方法について考慮する
2. 組織のリスクとレピュテーションへの影響を評価する
3. 潜在的な新たな脅威に対する主要な影響範囲を監視する
4. 既知または未知の脅威への対応方法を計画する

既知または未知の脅威への対応方法を計画する

AI の民主化は、コーディング経験がほとんどないが、悪意のある個人が利益のためにテクノロジーを悪用する可能性があるため、潜在的な脅威への扉を開きます。AI を活用した製品やサービスが個人にどのような影響を与えると予想されるかについては、多くのことが書かれています。イプソスの最近の調査では、雇用者の 57% が AI によって自分たちの働き方が変わると予期しており、36% が AI に完全に置き換わることを予期していることも示されています (Ipsos Global Views on AI)。

Q. 下記が、もしあるとしたら、その可能性はどのくらいだと思いますか



Base：22,816 人 (31 か国の 75 歳未満の成人)、2023 年 5 月 26 日から 6 月 9 日にかけて実施 -- インドを除くすべての国でオンラインのみ。
「世界の国平均」は、調査が実施されたすべての国の平均結果を反映しています（人口に合わせて調整されていません）。
Source：イプソス | AI 2023 に関する世界的な見解

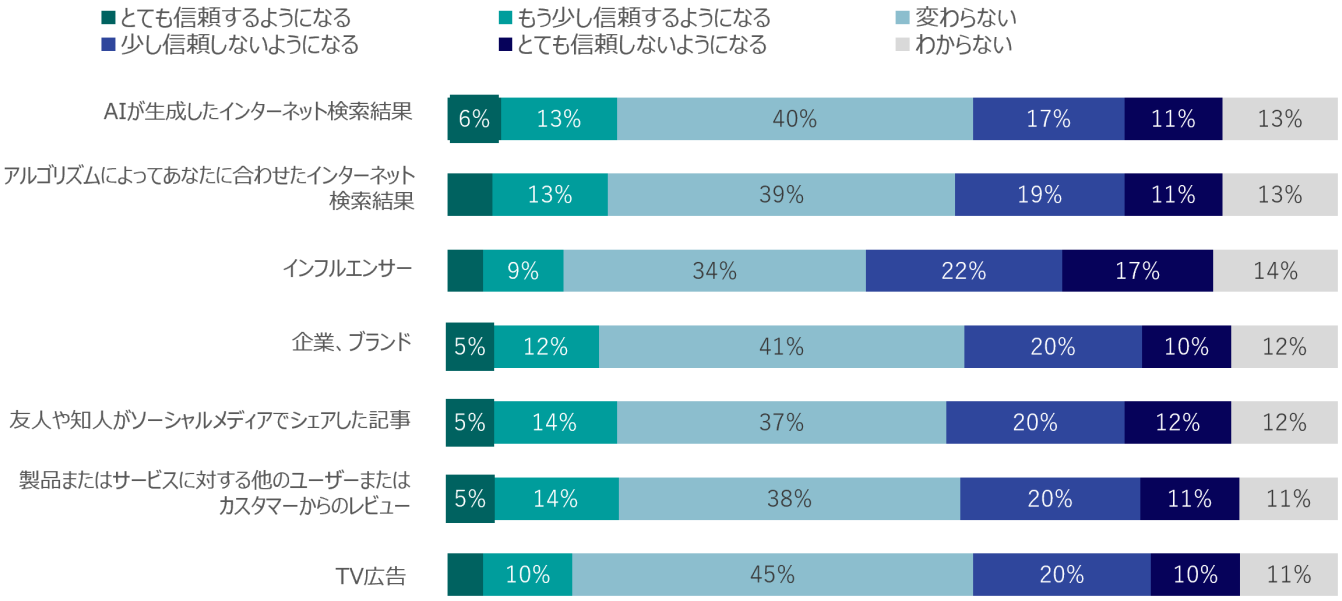
しかし、これらの進歩が企業に与える潜在的な悪影響や、企業のレピュテーションにどのような壊滅的な影響を与える可能性があるかについては、あまり議論されていません。例えば：

- **ソーシャル エンジニアリング攻撃**では、本物の人間の声と区別できない AI によって生成された人工音声を利用することができるため、詐欺師は企業幹部の声を模倣した詐欺を作成して、従業員をだまして機密情報を提供させたり、不正な金融取引を開始させたりすることができます。
- **画像捏造**によって、詐欺師が企業の幹部、業務、内部コミュニケーションに関係する架空のシナリオを描く写実的なビデオや画像を開発することができます。この新たな脅威は、否定的な認識を生み出し、重大な経済的損失につながることで、企業のレピュテーションに深刻なダメージを与える可能性があります。
- **フィッシングや詐欺**は、高度なビジネス電子メール侵害 (BEC) 攻撃の開始を支援する WormGPT などのツールによって強化されます。AI を活用した技術により、犯罪者は音声やビデオのマスキングを使用して、より説得力のあるパーソナライズされた詐欺を簡単に作成できるようになり、検出が困難になりました。そのため、詐欺はもはや従来の手段に限定されなくなりました。内部的には、生成 AI ツールによる攻撃は従業員を欺き、有害で不正確な情報を広め、社内にパニックや動揺を引き起こし、企業危機に対処する際の対応時間に影響を与える可能性があります。

外部的には、このような侵入は企業コミュニケーションの信頼を損ない、経済的損失やブランドのレピュテーションに対する回復不能な損害につながる可能性があります。

人々はAIが作成したコンテンツに不信感を持つ可能性が高い

Q. もし AI が下記によって、もっと広く使われるようになったら、それらに対して信頼感は変わりますか？



Base：1,109 名(アメリカの成人)、2023 年 2 月 14 日から 15 日にかけて実施　Source: Ipsos Consumer Tracker

組織のリスクとレピュテーションへの影響を評価する

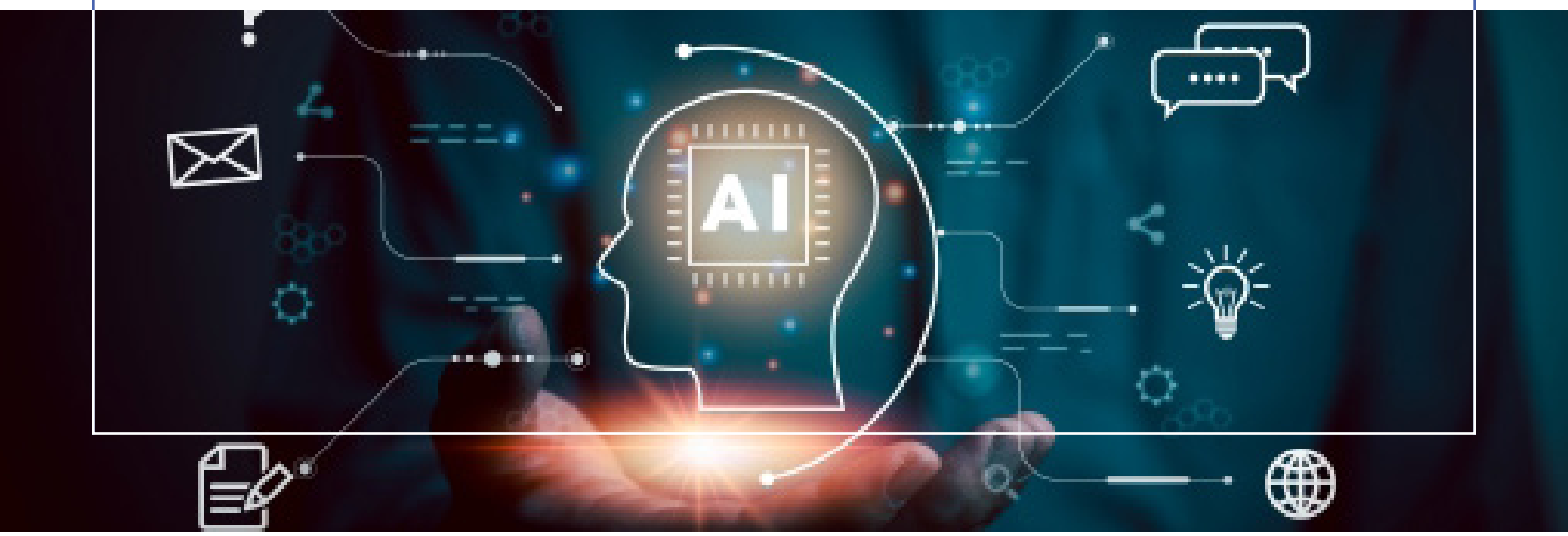
AI が生成する脅威に関連するリスクを効果的に軽減するには、企業はまず自社のビジネスとレピュテーションに対する潜在的な影響を特定し、優先順位を付ける必要があります。包括的なリスク評価は、脆弱性がどこにあるのかを理解し、緩和するためのカスタマイズされた戦略を開発するために不可欠です。

- **脆弱性の特定:** 企業は、現在の技術状況、データ セキュリティ プロトコル、および通信チャネルについて詳細な評価を実施する必要があります。潜在的な脆弱性点を特定することで、組織は AI のリスクに対して的を絞った防御を実装できるようになります。
- **AI の悪用の理解:** 生成 AI がどのように悪用されるかを理解することで、企業は潜在的な脅威をより適切に予測し、対処できるようになります。AI テクノロジーの最新の開発とその潜在的なリスクについて最新の情報を入手することは、プロアクティブなリスク管理戦略を開発するために不可欠です。
- **将来の脅威の予測:** 企業は、AI テクノロジーがどのように進化し、将来悪用される可能性があるかを先を見据えて予測し続ける必要があります。先進的なアプローチを採用することで、組織は潜在的な脅威に先手を打ち、対応する準備を整えることができます。

主要な影響領域を監視する

潜在的なリスクを特定した後、企業はこれらの AI による脅威を長期にわたって継続的に監視するための包括的なツールキットを確立する必要があります。このツールキットは 3 つの重要なコンポーネントで構成されます。

- **AI ベースの脅威検出:** AI テクノロジーを防御に活用します。組織は、レピュテーションの変化を監視するのに役立つデータを特定し、監視ツールへのほぼリアルタイムのデータ フィードを設定し、特に重要な指標における異常なイベントを監視する AI または大規模言語モデルをトレーニングする必要があります。
- **人間の監視:** AI は特定のリスクや主要指標の変化を検出するのに効果的ですが、依然として人間の監視が重要です。専門家チームは複数のデータ ストリームを監視し、AI によって生成されたコンテンツを検証して、正規のコンテンツと悪意のあるコンテンツを区別する必要があります。
- **協力的パートナーシップ:** AI 研究機関、サイバーセキュリティの専門家、レピュテーションとテクノロジーのリーダーとの協力に取り組みます。このようなパートナーシップは、新たなリスクに対処するための知識の共有と集団的な取り組みを促進します。



対応方法を計画する

AI 関連のリスクと機会に効果的に対処するには、企業は社内に専門のタスクフォースを設立する必要があります。このチームは、AI、データ サイエンス、サイバーセキュリティ、ポリシー、コミュニケーションの専門知識を持つ個人で構成される必要があります。AI タスクフォースの主な責任は次のとおりです。

- **リスク管理:** AI による潜在的なリスクを特定、分析、優先順位付けし、これらの脅威を効果的に軽減する戦略を策定します。
- **教育とトレーニング:** 組織全体で AI リテラシーの文化を育みます。AI が生成する脅威を認識して対応するためのトレーニングを従業員に提供します。
- **危機対応:** AI 関連のレピュテーションに関する緊急事態に迅速に対処するため、危機対応計画を作成およびリハーサルします。

著者:

Rhett Skelton
SVP, Ipsos Corporate Reputation
Rhett.Skelton@Ipsos.com

Michael McMenemy
Director, Ipsos Corporate Reputation
Michael.Mcmenemy@Ipsos.com

Jonathan Newton
Account Manager, Ipsos Corporate Reputation
Jonathan.Newton@Ipsos.com

イプソスについて

イプソスは世界有数の市場調査会社です。90カ国の拠点、100以上の市場で調査を実施しています。18,000人以上の従業員は、市場、ブランド、社会、そして生活者に対する溢れる好奇心を持っています。

クライアントのみなさまがより速く、より賢く、より大胆に行動できるように、情報と分析を提供します。

1975年にフランスで設立したイプソスは、リサーチのプロフェッショナルによって管理・運営されています。