SMBC
SMBCグループ
協力　日本実業出版社
SMBCコンサルティング
NETPRESS
2026.5.18
第2511号

【ＡＩを企業として導入するための第一歩】

生成ＡＩ利用ルールの策定で押さえておくべきポイント

さくら情報システム株式会社
プラットフォーム事業本部
セキュリティソリューション部
富田　愛美

Point

1. 企業の生成AI活用には、リスク管理と明確な利用ルール策定が不可欠です。
2. 利用目的や禁止事項、入力・出力情報の取り扱いを明示し、従業員が遵守することが重要です。
3. 定期的なルール見直しや技術対策も取り入れ、安全かつ効果的な運用を心掛けましょう。

1. 生成AIの導入状況

近年、生成AIの市場は技術の進歩が目覚ましく、群雄割拠の状況です。身近な例では、Microsoft EdgeやGoogleなどの検索エンジンに、AIが回答を生成する機能が導入され、日々の生活で利用している方も多いのではないでしょうか。

総務省の「令和7年版 情報通信白書」によると、生成AIを利用する企業が前年度と比較して増加傾向にあります。一方で、中小企業に着目すると、「効果的な活用方法がわからない」「情報漏えい等のセキュリティリスクがある」といった理由から、導入・活用が十分に進んでいない状況です。実際に、企業における生成AIの利用には、社内情報の漏えい、著作権等の権利侵害、事実と異なる情報の生成による誤った判断など、さまざまなリスクが存在します。そのため、企業内で安全に生成AIを利用するには、まず、生成AI利用に関するルールを策定することが重要です。

2. 安全に利用するためのルール策定のポイント

企業内の生成AI利用に関するルール策定において、ポイントは大きく次の3つがあります。

(1)	生成AIの利用目的・用途、禁止事項を定める
(2)	入力してよい情報と、入力してはいけない情報を明示する
(3)	出力結果の妥当性や正確性を必ず確認する

これら3つのポイントを踏まえた生成AIの利用ルールを策定し、遵守することで、生成AI利用に伴うリスクを低減することができます。生成AI特有の注意点もありますが、基本的にはインターネット上で機密情報を取り扱う際の基本的なポイントを守ることで、安全かつ適切に利用することが可能です。以下、各ポイントについて詳しくみていきましょう。

(1) 生成AIの利用目的・用途、禁止事項を定める

①利用する目的や使用用途を明確に定める

どの生成AIをどの業務に使用してよいか、また使用してはいけない業務が何かを具体的に示すことで、従業員は迷うことなく生成AIを活用でき、企業全体での生成AI利用の促進につながります。さらに、情報漏えいなどのリスクを防ぐためにも、生成AIの私的利用（目的外利用）を抑制するルールを設けることが重要です。生成AIによっては、生成物の権利帰属（商用利用の可否）が利用規約で定められている場合がありますので、注意が必要です。

（次頁に続く）

②生成AIの利用にあたっての禁止事項を定める

生成AIの利用目的・用途から外れた利用は当然禁止されますが、目的内の利用であっても、企業の社会的信用を損なう行為については、明確に禁止事項としてルールに盛り込む必要があります。主な禁止事項は以下の通りです。

・個人のプライバシーを毀損するリスクのあるコンテンツの作成

・違法行為やハラスメントを促進・助長するコンテンツの作成

・誤った情報の提供や、個人を意図的に欺くことを目的としたコンテンツの作成

このような禁止事項を社内ルールに明記し、生成AIの適切な利用を徹底し、企業の社会的信用や倫理的責任を守ることが重要です。

(2) 入力してよい情報と、入力してはいけない情報を明示する

生成AIに入力したデータは、AIモデルの学習用データとして利用される場合があり、重要情報を入力するとプライバシーの侵害や情報漏えいにつながるリスクがあります。そのため、「著作権保護の対象となる情報」「個人情報」「組織の機密情報（顧客情報を含みます）」などは入力を禁止するなど、ルールとして制限する必要があります。

特に企業利用の場合、他社との間で守秘義務がある情報や、顧客から預かっているデータを生成AIに入力することは、契約違反となる可能性があるため、十分な注意が必要です。

(3) 出力結果の妥当性や正確性を必ず確認する

入力データだけではなく、生成物（AIの出力結果）の取り扱いにも十分な注意が必要です。生成物には、ハルシネーションと呼ばれる事実と異なる情報が含まれる可能性があります。現実には存在しない情報や誤った内容が含まれていないか、利用者自身が責任をもって、生成物の妥当性・正確性を裏付けることが重要です。また、生成AIの学習に使用されるデータの偏りによって、意図せず不公平な判断が生じるAIバイアスにも注意が必要です。

出力結果を利用する際は、根拠や裏付けを必ず確認し、リスクや出力結果の妥当性・正確性を判断する責任が利用者自身にあることを認識してください。

3. 導入時に気を付けるべきポイント

生成AIの導入時に気を付けておきたいポイントをいくつか紹介します。

(1) オプトアウトできるサービスを選択する

生成AIの「オプトアウト」とは、利用者が入力したデータをAIモデルの学習に利用されないようにする設定です。オプトアウトができないサービスで、個人情報や顧客情報などの重要情報を入力してしまうと、データが学習に使われ、プライバシー侵害や情報漏えいのリスクがあります。

(2) 秘密保持契約（NDA）を結ぶ

オプトアウト設定をしても、入力データはログとして生成AIの提供元に残る場合があります。提供元からの情報漏えいや目的外利用を防ぐためにも、NDAを締結することが重要です。

(3) 生成AIの入力制御機能を活用する

入力データについて、たとえば、電話番号などの個人情報の入力を技術的に制御する「ガードレール」機能をもつサービスもあります。ルールの設定に加えて、技術的な制御が可能かどうかもサービス選定時の要件として確認しましょう。

4. 終わりに

生成AIを安全に企業で活用するためには、まず「利用ルールの策定」と、そのルールを確実に運用することが不可欠です。加えて、従業員が内容を正しく理解し、日常業務で確実に守ることも重要になります。

また、生成AIは日々進化しており、技術や社会的な要請も変化し続けています。そのため、現状に合わせて、ルールの定期的な見直し・更新を行うことも安全な運用には欠かせません。

ぜひ、これらのポイントを意識しながら、生成AIを安全かつ効果的に活用してください。

本稿に関するご照会窓口
SMBCコンサルティング
ソリューション開発部　経営相談グループ
TEL:0120-874-809