

2024年度 JUAS AI研究会  
Cグループ ブレーキチーム  
～生成AIガイドラインに新解釈を加える～

Jフェス成果報告資料(別紙) 成果物

2025年4月

一般社団法人 日本情報システム・ユーザ協会 2024年度 AI研究会  
Cチーム

企業において言語系生成AIの導入が進む中で、その活用ガイドラインの参考として「日本ディープラーニング協会 (JDLA)生成AIの利用ガイドライン」が多くの企業で利用されています。



## ガイドライン作成目的

- 『生成AIの活用を考える組織がスムーズに導入を行える』ようになること
- 『このひな型を用いることによって生成AIの利活用の促進、ひいては産業・社会実装が進んでいくこと』

出典:生成AIの利用ガイドラインの作成にあたって(一般社団法人日本ディープラーニング協会)

## ガイドライン活用例 (参考資料としてJDLAガイドラインが明記・紹介されているもの)



千葉県  
生成AI利用のガイドライン

上智大学  
教育における生成AI利用に関するガイドライン



日本ディープラーニング協会  
生成AIの利用ガイドライン

当研究会では、日本ディープラーニング協会(JDLA)の生成AIガイドラインを基盤とし、より使いやすく、かつ効果的なガイドラインの策定を通じて、生成AIの利用促進と、ルール遵守の徹底を図ることを目指しました。これにより、企業や組織における生成AI活用の円滑化と、関連する課題の解決につながることを期待します。

## 問題点

禁止事項ばかり記載されている

著作権に偏ったリスクの説明に終始している

法律の条項をそのまま引用した／専門用語が多いこと  
で読解のハードルが高い

文字のみで読み手の興味を引かない／理解しづらい

ユースケースの記載が無く、利用者が活用イメージ  
をつかめない

生成AI自体の説明がない



利用促進のための  
ガイドラインとするには？

## 改善点

専門用語を簡略化し  
具体例を追加して理解しやすくする

利用者目線で社内に合った  
ユースケースや具体例を明示する

別冊で図表サンプルを掲載することで  
理解を助ける

新解釈！

# 生成AI利用ガイドライン

第1.0版

令和7年3月

一般社団法人日本システムユーザ協会 AI研究会 Cチーム

1. 生成AIについて	...	3ページ
生成AIの概要	...	4ページ
2. 生成AIがもたらすリスク	...	5ページ
生成AI利用の5つのリスク	...	6ページ
知的財産権のリスク	...	7ページ
個人情報侵害のリスク	...	13ページ
虚偽のリスク	...	16ページ
差別・偏りのリスク	...	18ページ
権利保護が行われないリスク	...	20ページ
3. 今後の生成AI利活用について	...	22ページ
4. 参照先	...	28ページ
5. Appendix	...	30ページ

# 1. 生成AIについて

## 生成AIの特徴

### 1. 新しいコンテンツを生成する技術です！

- 生成AIは、画像、音楽、テキストなど、新しいデジタルコンテンツを自動で作り出す技術です。

### 2. 様々な分野での活用されています！

- この技術は、アート、エンターテインメント、広告、さらには研究領域に至るまで、多岐にわたる分野で活用されています。

### 3. 創造性と革新を促進します！

- 生成AIは、従来の方法では考えられなかったような新しいアイデアやコンセプトを創出し、創造的なプロセスを加速します。



簡単に言うと・・・  
生成AIは、「新しいものを作り出すロボットの頭脳」のようなものだよ。

例えば、絵を描いたり、お話を書いたり、人とお話する文章を考えたりすることができるんだ。まるで、お絵かきが得意な友達や、お話を考えるのが上手な先生が、パソコンの中にいるみたいだね。

でも、このAIは自分で考えているわけではなく、たくさんのデータを学んで、それをもとに新しいものを作っているんだ。だから、間違えたり、ちょっと変なことを言ったりすることもあるよ。

私たちが上手に使えば、宿題を手伝ってくれたり、おもしろいお話を作ったり、みんなの仕事を助けたりすることができるんだよ！



## 2. 生成AIがもたらすリスク



# 生成AI利用の5つのリスク

2024年度  
JUAS AI研究会

生成AIの利用には、大きく以下の5つのリスクが存在します。



## 知的財産権侵害

- 第三者が著作権を有しているデータ
- 登録商標・意匠
- 他社から秘密保持義務を課されて開示された秘密情報
- 自組織の機密情報



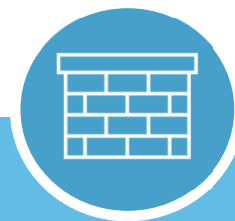
## 個人情報侵害

- 著名人の顔写真や氏名の無許可利用
- 個人情報の目的外利用



## 虚偽

- 生成物の内容に虚偽が含まれている可能性がある



## 差別・偏り

- 生成物の内容が基本的人権を尊重しない可能性がある



## 権利保護が行われない

- 生成物は知的財産権が発生しない

想定されるリスク

## 知的財産権侵害のリスク

# (1) 第三者が著作権を有しているデータ（他人が作成した文章等）

2024年度  
JUAS AI研究会

単にAIに他人の作品を入力するだけでは、一般的には著作権を侵しているとはみなされません。しかし、その入力によって、他人の作品とほとんど同じか、非常に似た作品を作ることを目的としている場合、その行為自体が著作権の侵害と判断される可能性があります。

出典: 令和5年度 著作権セミナー AIと著作権 2023年6月 文化庁著作権課

## Goodケース

競合他社の広告文を生成AIに入力し、「この広告文の内容を要約し、どのようなマーケティング戦略が使われているか分析してほしい」と依頼する。



この広告文の内容を要約し、  
どのようなマーケティング戦略が  
使われているか分析して。

生成AIの生成物については、入力者自身が内容を適切に評価・編集し、適切な引用に留めてください。

## Badケース

競合他社の広告文の一部を生成AIに入力し、「この広告文と同じような文章を新しく作ってほしい」と依頼する。



この広告文と同じような文章を  
新しく作って。

意図的に競合他社の模倣品を作成しようとしているため、NG行為です。  
既存の著作物に類似させるような指示はやめましょう。

## (2) 登録商標・意匠（ロゴやデザイン）

2024年度  
JUAS AI研究会

商標や意匠として登録されているロゴやデザインを生成AIに入力するだけでは、商標権や意匠権を侵害したことにはなりません。ただし、誰かの登録されたロゴやデザインと全く同じか、非常に似たものをわざと作って、それを商用利用する場合は、権利を侵害する可能性があります。

出典: AI 時代の知的財産権検討会 中間とりまとめ 2024 年5月 AI 時代の知的財産権検討会

### Goodケース

競合他社のロゴやデザインを、あくまで「参考資料」として、生成AIに入力し、共通して使われている色使いや形状、レイアウトの特徴などを抽出する。



このロゴの色使いや形状の特徴を調べて。

生成物の二次利用には注意が必要です。入力者自身が内容を適切に評価・編集し、適切な引用に留めてください。

### Badケース

競合他社のロゴを生成AIに入力し、「このロゴに似たデザインを作ってほしい」と依頼する。



このロゴと同じようなデザインを新しく作って。

有名なロゴを故意に入力し、その生成AIの成果物を使って他者を誤認させる等、悪意のある行為をしてはいけません。既存の商標・意匠に類似させるような指示はやめましょう。

### (3) 他社から秘密保持義務を課されて開示された秘密情報

2024年度  
JUAS AI研究会

自分の仕事を助けるために翻訳したり、文章を分かりやすく直したりする行為は、秘密保持義務に違反するものではありません。しかし、生成AIを使って次のようなことをすると、秘密保持義務に違反する可能性があります。

<具体例>

- ・第三者がアクセス可能なホームページ上にデータを掲載する
- ・大量のデータをタブレットやスマートフォンの画面に表示し、それを第三者に見せる
- ・取得したデータを使って研究・開発する
- ・取得したデータを使って物品を製造し、又は、プログラムを作成する
- ・取得したデータからAI技術を利用したソフトウェアの開発(学習)

出典:「秘密情報の保護ハンドブック」・「限定提供データの指針」における 生成AIに関する記載部分 2024年3月 経済産業省知的財産政策室

### (3) 他社から秘密保持義務を課されて開示された秘密情報

2024年度  
JUAS AI研究会

#### Goodケース

取引先から提供された技術文書(英語)を、自身の理解の助けのために日本語に翻訳させる。



この技術文書を翻訳して

問題ありません。

#### Badケース

取引先から提供されたプログラムコードを、「取引先の許可なく」解析し、コードの模倣を依頼する。



このプログラムを解析して、同じ機能だが別のコードに書き換えて

取引先との合意事項を無視して生成AIツールを使用してはいけません。

## (4) 自組織の機密情報

2024年度  
JUAS AI研究会

自社内の機密情報(ノウハウ等)を生成AIに入力する行為は、機密情報の漏えいではありません。ただし、担当部署が指定していない生成AIを使うと、AIの処理方法や利用規約の内容によっては、機密情報が保護されなくなったり、特許出願ができなくなったりするリスクがあります。必ず担当部署に相談してください。

出典:「秘密情報の保護ハンドブック」・「限定提供データの指針」における 生成AIに関する記載部分 2024年3月 経済産業省知的財産政策室

### Goodケース

自社の機密にあたる販売戦略会議の議事録を、自社内で利用を許可された生成AIツールを利用し、要約する。



この議事録を要約して。

社内で許可された生成AIツールを利用する場合は問題ありません。

### Badケース

自社の機密にあたる販売戦略会議の議事録を、社外(自社で許可されていない)の生成AIツールで利用し、要約する。



この議事録を要約して。

許可されていない生成AIツールを使用すると、入力した情報が学習され、二次利用されてしまう可能性があります。

自社内の機密情報を入力する必要がある場合は、社内で許可された生成AI環境を利用しましょう。

想定されるリスク

## 個人情報侵害のリスク



# (1) 著名人の顔写真や氏名の無許可利用

2024年度  
JUAS AI研究会

著名人の顔写真や名前を生成AIに入力するだけでは、その著名人のパブリシティ権(肖像権などに近い権利)を侵害することにはなりません。しかし、その画像や名前を商用利用する場合は、パブリシティ権を侵害する可能性があります。

出典: AI時代の知的財産権検討会 中間とりまとめ 2024年5月 AI時代の知的財産権検討会

## Goodケース

マーケティング用に、著名人の顔写真や名前を生成AIに入力して、内部資料用に著名人のイメージやプロフィールの分析レポートを作成する。



著名人のイメージやプロフィールの分析レポートを作成して。

内部資料として使用する分にはパブリシティ権侵害になりません。ただし、社外向けに利用する場合は、パブリシティ権侵害になる可能性があるので、注意が必要です。

## Badケース

著名人の顔写真を生成AIに入力して作成した画像を、企業の広告キャンペーンに無断で使用する。



この著名人の顔写真から画像を作成して。

無断で著名人の顔写真や名前を商用利用することはパブリシティ権侵害となる可能性があります。

商用利用する場合は、許可を得て使用しましょう。

## (2) 個人情報の目的外利用

2024年度  
JUAS AI研究会

集めた個人情報を、その情報を集めた目的のためだけに生成AIに入力する行動は、個人情報のルールに反することはありません。しかし、収集目的以外に使ってしまうと、個人情報保護法に違反する可能性があります。

出典:生成AIサービスの利用に関する注意喚起等 2023年6月 個人情報保護委員会

### Goodケース

顧客アンケートで収集した個人情報を、あらかじめ設定した顧客満足度向上の目的に沿って、社内専用の生成AIツールで解析する。



この顧客アンケートを分析して。

収集目的に沿った用途で個人情報を利用することは問題ありません。  
生成AIの生成した結果の扱いには十分注意が必要です。

### Badケース

顧客満足度向上の目的で収集した顧客アンケートの個人情報を、社内の人事評価等、別の利用目的で生成AIに分析させ、その結果を使用する。



この顧客アンケートを分析して、  
社内で同一人物がいたら査定  
に評価を加えて。

収集目的と異なる用途で個人情報を利用してはいけません。  
個人情報は、個人情報保護法に準じて利用しましょう。

想定されるリスク  
**虚偽のリスク**

# (1) 生成物の内容に虚偽が含まれている可能性がある

2024年度  
JUAS AI研究会

大規模言語モデルは、ある単語の後に一番出る可能性が高い単語を順番に選んで、自然な文章を作り出す仕組みです。そのため、文章には間違いが含まれていることがあります。生成された内容は、必ず自分でチェックして、正しいかどうかを判断してください。

出典:生成AIサービスの利用に関する注意喚起等 2023年6月 個人情報保護委員会

## ➡ 注意すべき点

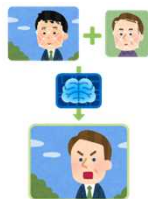
- ✓ 生成された内容は必ず確認する



生成された内容は、必ずしも正しい情報とは限りません。  
生成された結果の正確性については、利用者自身の責任で必ず確認しましょう。

文法は正しいが内容が誤っている例:  
エジプトのピラミッドは、古代にアメリカ人によって建設されました。

- ✓ 信頼できる情報か否か確認する



ディープフェイクなど存在しない事実や発言をあたかも本物の証拠として生成している場合があります。  
安易に誤情報に騙されないよう、信頼できる情報が確認するようにしましょう。

想定されるリスク

## 差別・偏りのリスク

# (1) 生成物の内容が基本的人権を尊重しない可能性がある

2024年度  
JUAS AI研究会

生成AIは、学習データをもとに動いているため、もしそのデータに偏りがあれば、その偏りがAIの判断にも影響を与えることがあります。たとえば、国籍、人種、性別などについての偏った学習データがあれば、AIも似た偏りを持つ可能性があります。生成された内容は必ず自分で確認し、正しいかどうか判断してください。

出典：生成AIサービスの利用に関する注意喚起等 2023年6月 個人情報保護委員会

## ➡ 注意すべき点

- ✓ バイアスや偏見が含まれていないか確認しましょう



人種や性別、年齢などに対して不利益や偏見をもたらす先入観が含まれている可能性があります。  
過去にバイアスが問題になった事例と類似していないか調べるなどして、バイアス・偏見の有無を確認しましょう。

バイアス・偏見の例：

特定の人種の若者は犯罪に走りやすいと結論付ける。

個人が持つ属性情報は性別以外、全て同一にも関わらず、性別の差異でローン審査の結果を変える。

想定されるリスク

**権利保護が行われないリスク**

# (1) 生成物は知的財産権が発生しない

2024年度  
JUAS AI研究会

生成AIは人間ではないので、AIが作った生成物自体には通常、著作権や特許などの知的財産権は発生しません。ただし、例えば著作権の場合は、その生成物に人間がどれだけ創作的な工夫を加えたかで判断が分かります。権利を主張したい場合は、AIの生成物をそのまま使うのではなく、自分で加筆や修正を加えるようにしましょう。

出典: AI時代の知的財産権検討会 中間とりまとめ 2024年5月 AI時代の知的財産権検討会

## ➡ 注意すべき点

- ✓ AIの生成物には、自分で加筆・修正を行い人間の創作を加えましょう



AIが作った生成物には知的財産権は発生しません。  
知的財産権を主張する必要がある生成物は、自身の手で加筆・修正しましょう。



## 3. 今後の生成AI利活用について

## 生成AIの未来と社会への影響

### 概要

- 生成AIは技術革新を加速させ、あらゆる業界での業務効率化を促進する
- 企業の競争力向上、個人の生産性向上、創造的な活動の支援が期待される
- 一方で、倫理的課題やセキュリティリスクへの対応が求められる



### 主な影響

- 業務効率化と自動化により、ルーチン作業が削減され、人間は創造的な業務に集中可能となる
- AIによるデータ分析と予測が迅速な判断を支援し、意思決定が高度化される
- フェイク情報の生成、プライバシー侵害、バイアスなどの新たなリスクが出現する

### 今後の展望

- 生成AIの適正利用を促進するガイドラインの整備の重要性が増す
- 人間とAIの協調による新たな働き方の確立され、社会に貢献できる環境が整えられる
- 継続的な技術進化と社会受容のバランスが重要視される

## 生成AIとDevSecOps ～セキュリティと効率の向上～

### 課題

- 開発、セキュリティ、運用の統合が進む中で、脆弱性対応の迅速化が求められる
- 手動でのセキュリティチェックやコードレビューは時間がかかる
- 開発者とセキュリティチームの間で認識のズレが発生しやすい

### 生成AIの活用

- 自動コードレビューと脆弱性検出: AIがソースコードを解析し、潜在的な脆弱性を指摘
- セキュリティポリシーの適用支援: コード変更時に自動的にベストプラクティスに沿った対応を提案
- リアルタイムのフィードバック: 開発者がコーディング中に、セキュリティの問題を即時指摘

### 期待される効果

- セキュリティを組み込んだ迅速な開発の実現
- 開発者のセキュリティ意識の向上
- 脆弱性修正の効率化と対応スピードの向上

## 脅威インテリジェンスへの活用

### 課題

- 脅威インテリジェンスの情報量が膨大で、分析に時間がかかる
- レポートの解読に専門知識が必要になる
- 迅速な意思決定のための情報整理が困難になる

### 生成AIの活用

- 自動要約: 大量の脅威レポートを解析し、要点を抽出
- 多言語翻訳: 海外の最新情報を即座に翻訳・要約
- リスク評価の補助: AIが脅威の深刻度を分析し、優先度付けを支援

### 期待される効果

- 分析時間の短縮と対応スピードの向上
- インテリジェンスの理解・活用のしやすさ向上
- 情報の網羅性と正確性の向上

## セキュリティ教育

### 課題

- 従業員のセキュリティ意識の向上が課題となる
- 既存の研修は受動的で理解が進みにくい
- 実践的なトレーニングが不足している

### 生成AIの活用

- チャットボットによる対話型学習：実際の攻撃シナリオを模擬し、リアルタイムでフィードバック
- カスタマイズ可能な演習：役職や職務に応じた学習内容を提供
- 継続的な学習支援：日常業務の中で簡単な問題を出題し、意識向上を図る

### 期待される効果

- より実践的で効果的なセキュリティ教育の提供
- 全従業員のセキュリティリテラシー向上
- インシデント発生時の適切な初動対応の促進

## ログ分析と異常検知の効率化

### 課題

- セキュリティログのデータ量が膨大で、分析が困難になる
- 誤検知・過検知が多く、適切な対応が難しい
- インシデントの兆候を見逃すリスクがある

### 生成AIの活用

- パターン認識と異常検知: AIが通常の動作パターンを学習し、不審な活動を自動検知
- 説明可能な分析結果: AIが検出した異常の根拠を明示し、判断を支援
- 優先度付けの自動化: インシデントの深刻度をAIが評価し、迅速な対応を可能に

### 期待される効果

- SOC(セキュリティオペレーションセンター)の負担軽減
- 誤検知の削減と対応精度の向上
- 早期発見による被害の最小化

## 4. 参照先

生成AIの利用にあたって、不明点等あれば以下の連絡先へ照会してください。

問い合わせ内容	担当者	問い合わせ先/参照URL
全般的な利用に関すること	〇〇部〇〇担当	メールアドレス
		URL
データ・セキュリティに関すること	△△△部△△△担当	メールアドレス
		URL
品質・信頼性に関すること	□□部□□□担当	メールアドレス
		URL
技術サポートに関すること	※※※部※※担当	メールアドレス
		URL



# 5. APPENDIX

# 参考文献(1)

2024年度  
JUAS AI研究会

当ガイドライン作成にあたって、参考としたガイドライン等は以下のとおりです。適宜参照してください。

ガイドライン	発行主体	主なポイント	参照URL
生成AIの利用ガイドライン	一般社団法人 日本ディープラーニング協会(JDLA)	<ul style="list-style-type: none"><li>◆ 導入支援</li><li>◆ 組織内調整の促進</li><li>◆ 最新情報の提供</li></ul>	<a href="#">JDLA ガイドライン</a>
AI事業者ガイドライン	経済産業省	<ul style="list-style-type: none"><li>◆ 包括的な指針</li><li>◆ 基本理念の提示</li><li>◆ 具体的な取り組み</li></ul>	<a href="#">AI 事業者ガイドライン(第 1.0 版)</a>
テキスト生成AI利活用におけるリスクへの対策ガイドブック	デジタル庁	<ul style="list-style-type: none"><li>◆ 行政向けの指針</li><li>◆ 具体的なリスク対策</li><li>◆ 最新の動向反映</li></ul>	<a href="#">テキスト生成AI利活用におけるリスクへの対策ガイドブック(α版)</a>
テキスト生成AIの導入・運用ガイドライン	情報処理推進機構(IPA)	<ul style="list-style-type: none"><li>◆ 実践的な指針</li><li>◆ リスク管理</li><li>◆ 事例紹介</li></ul>	<a href="#">テキスト生成AIの導入・運用ガイドライン</a>

## 参考文献(2)

2024年度  
JUAS AI研究会

当ガイドライン作成にあたって、参考としたガイドライン等は以下のとおりです。適宜参照してください。

ガイドライン	発行主体	主なポイント	参照URL
文章生成AI利活用ガイドライン	東京都デジタルサービス局	<ul style="list-style-type: none"><li>◆ 生成AIの業務活用とリスク</li><li>◆ 安全な利用環境の整備</li><li>◆ 利用上のルール遵守</li></ul>	<a href="#">文章生成AI利活用ガイドライン・活用事例集   ICT導入・活用の推進   東京都デジタルサービス局</a>
千葉県 生成AIの利用ガイドライン	千葉県	<ul style="list-style-type: none"><li>◆ 業務利用の明確化</li><li>◆ 具体的な注意点の提示</li></ul>	<a href="#">千葉県 生成AIの利用ガイドライン 第2.0版</a>
生成AIの利用ガイドライン作成のための手引き	STORIA法律事務所	<ul style="list-style-type: none"><li>◆ 法的リスクの明確化</li><li>◆ 多様な利用者への対応</li><li>◆ 具体的なサービス対象</li></ul>	<a href="#">生成AIの利用ガイドライン作成のための手引き - STORIA法律事務所</a>
Fujitsu 生成AI利活用ガイドライン	富士通株式会社	<ul style="list-style-type: none"><li>◆ 社内展開の実績</li><li>◆ リスクと対策の明確化</li><li>◆ 実用的な内容</li></ul>	<a href="#">企業利用のリスクと対策例を解説「生成AI利活用ガイドライン」を一般公開</a>
医療・ヘルスケア分野における生成AI利用ガイドライン	非営利公益法人 医療AIプラットフォーム技術研究組合	<ul style="list-style-type: none"><li>◆ 医療現場でのリスク対策</li><li>◆ 具体的な利用シナリオ</li><li>◆ 最新の研究成果の反映</li></ul>	<a href="#">医療・ヘルスケア分野における生成AI利用ガイドライン - HAIP</a>

## 参考文献(3)

当ガイドライン作成にあたって、参考としたガイドライン等は以下のとおりです。適宜参照してください。

ガイドライン	発行主体	主なポイント	参照URL
武蔵野大学 教職員向け生成AIの利用ガイドライン	武蔵野大学	<ul style="list-style-type: none"><li>◆ 明確な目的設定</li><li>◆ 具体的な対象AIの明示</li><li>◆ 法令遵守の強調</li></ul>	<a href="#">武蔵野大学 教職員向け 生成AIの利用ガイドライン</a>
教育における生成AI利用に関するガイドライン	上智大学	<ul style="list-style-type: none"><li>◆ 生成AI利用の指針</li><li>◆ 授業・課題での使用可否明示</li><li>◆ 倫理/法/社会的問題への注意喚起</li></ul>	<a href="#">教育における生成AI利用に関するガイドライン</a>
責任あるAIとルール	古川 直裕・吉永京子 一般社団法人 金融財政事情研究会	<ul style="list-style-type: none"><li>◆ EU・米国の価値観の理解</li><li>◆ リスクの整理と具体的な対策</li><li>◆ 生成AIの推進体制・管理体制</li></ul>	-