



# 生成系AIにおけるプライバシー

一般社団法人

日本クラウドセキュリティアライアンス  
クラウドプライバシーWG リーダー山崎

# 講師紹介

- ユーザー系企業でオンラインシステムのSEとして業界入り。
- プリケーションPGM開発/設計⇒共通プログラム⇒システム周り(OS/DB/NW)⇒航空機搭載機器PGM⇒操縦マニュアル管理⇒法務部にてIT法やセキュリティに関する社内規程作成⇒セキュリティグループ創設⇒セキュアコーディングコース作成⇒コンプライアンス部創設⇒金商法対応(J-SOX対応)⇒BCP作成⇒東日本大震災では全社対応本部指揮⇒CSAにてプライバシー関連の行動規範(CoC)を翻訳・執筆(CoC)
- ISO27000審査員      ISACA/CRISC



# 個人情報とプライバシー

## 個人情報

生存する個人に関する情報で、氏名、生年月日、住所、顔写真などにより特定の個人を識別できる情報。他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものも含む。

個人情報保護法の定義

## プライバシー

個人や家庭内の私事・私生活。また、それを他の個人や社会に知られず、干渉を受けない権利。

個人情報保護の文脈では、他者が管理している自己の情報について訂正・削除を求めることができる権利（積極的プライバシー権）を指す。英語の privacy を片仮名表記したものであり、日本語では私事権と訳されることもある。

Wikiより

個人情報保護法、第23条安全管理措置/第32条保有個人データに関する事項の公表等～第40条個人情報取扱事業者による苦情の処理がプライバシーに関連する法規

# 生成系AIとは

- 簡単に言うと「何兆もの単語から構成される文章と、何千もの高性能なコンピュータチップを使って訓練された大規模言語モデル（LLM:Large Language Model）」
- 読み込ませた文章が知識ベースになる。
- 言語モデルとは入力文から予測して単語を出力するモデルです
  - 蕎麦屋-天ぷら蕎麦 レストラン-? ←ハンバーグ

# 最新の外国政府の動き 米国

- 人工知能（AI）の安心、安全で信頼できる開発と利用に関する大統領令  
Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligenceを2023/10/30に発令

- 1. 安全性とセキュリティーの新基準
- 2. 米国民のプライバシー保護
- 3. 公平性と公民権の推進
- 4. 消費者、患者、学生の権利保護
- 5. 労働者の支援
- 6. イノベーションと競争の促進
- 7. 外国における米国のリーダーシップの促進
- 8. 政府によるAIの責任ある効果的な利用の保証

議会に対し、全ての米国民、特に子供のプライバシー保護を強化するため、超党派のデータプライバシー法案を可決するよう求める。また、全米科学財団の実施する助成金事業「リサーチ・コーディネーション・ネットワーク」への資金提供を通じ、暗号ツールのような個人のプライバシーを保護する研究や技術を強化する。

<https://www.jetro.go.jp/biznews/2023/11/495833ae70119dbf.html>

JETRO  
日本貿易振興機構(ジェトロ) 海外ビジネス情報 サービス 国・地域別に見る 目的別に見る 産業別に見る

ビジネス短信

### バイデン米政権、AIの安全性に関する新基準などの大統領令公表

(米国)

2023年11月01日

米国のバイデン政権は10月30日、人工知能（AI）の安心、安全で信頼できる開発と利用に関する大統領令を発令した。今回の大統領令は、AIに関して、新たな安全性評価、公平性と公民権に関するガイドランス、AIが労働市場に与える影響に関する調査を義務付けるもので、米メディアの報道によれば、米国において初めての法的拘束力のある行政措置となる。グーグルやオープンAIなどのAI開発で先行する企業はこれまでに、AIの安全な開発のための自主的な取り組みを発表し、強制力のある規制が導入されるまでそれらを続けるとしていた（注）。

ホワイトハウスが同日に公開したファクトシートでは、大統領令の主要な構成要素を8つの項目に分けている。概要は次のとおりだ。

# 参考リンク

- 個人情報保護委員会 生成AIサービスの利用に関する注意喚起等について  
• [https://www.ppc.go.jp/news/careful\\_information/230602\\_AI\\_utilize\\_alert/](https://www.ppc.go.jp/news/careful_information/230602_AI_utilize_alert/)
- 東京都 文章生成AIの利活用に関するガイドライン  
• <https://www.metro.tokyo.lg.jp/tosei/hodohappyo/press/2023/08/23/14.html>
- 一般社団法人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  
• <https://www.jdla.org/document/#ai-guideline>
- PWC 生成AIを巡る米欧中の規制動向最前線  
• <https://www.pwc.com/jp/ja/knowledge/column/awareness-cyber-security/generative-ai-regulation.html>

# 個人情報を利用する時に必要な事

- 利用目的の通知・公表 法17条～法21条
  - 出来るだけ具体的に判りやすく記載が必要
  - 事業活動に用いるため/マーケティング活動に用いるため
    - 一般的には、業種の明示だけでは何に使われるかわからないので、個人情報の利用目的の特定があるとは認められません
  - **利用目的の変更**は変更前の利用目的と**関連性を有すると合理的に認められる範囲**を超えては行えない
    - 大きな利用目的の変更は本人からの**同意取得**が必要
  - **要配慮個人情報**を取得する場合は本人からの**同意取得**が必要

公表する段階で第三者提供まで同意していると解釈している

# 海外移転 法28条

- 日本国外へ個人情報に移転させること
  - EUと英国はこの適用の対象外
- 同意取得時に、移転先国の名称、移転先国における個人情報の保護に関する制度の有無等について本人に情報提供
- 移転先事業者の取扱い状況等の定期的な確認＋本人の求めに応じて関連情報を提供 (除くEUと英国)

個人情報の処理が行われなければ対象外

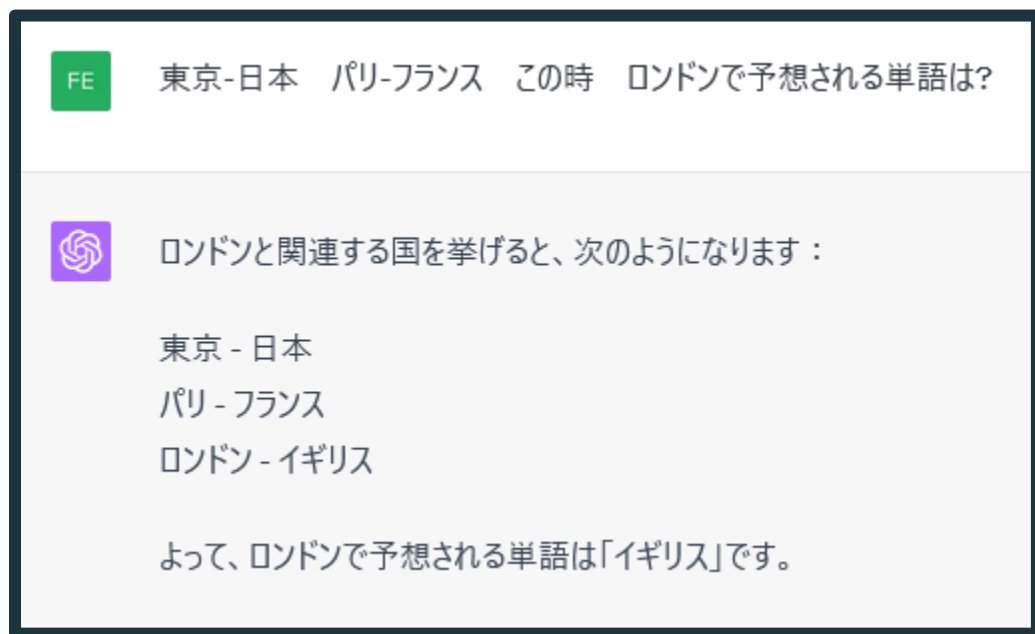


# 各法令・ガイドラインまとめ


- 教師データに個人情報が使われないようにする。
- データが越境移転する時の配慮/措置が必要
- 生成した結果は人間の確認が必要 判断を委ねない
  - 個人情報に関してはデータ主体の同意が得られているか確認が必要。
- 著作権に配慮した生成を実施

# プロンプト例

- 東京-日本          パリ-フランス          ロンドン-?   ←英国
- 東京とパリ      が前提ルールと解析し、ルールから英国と  
いう回答を導き出す。



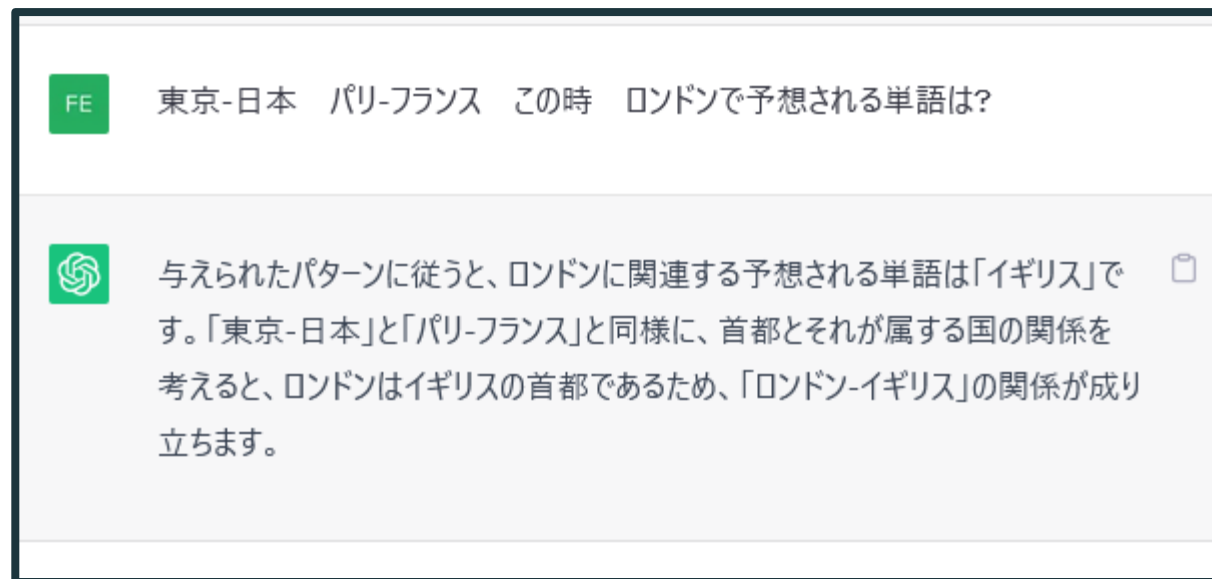
FE 東京-日本 パリ-フランス この時 ロンドンで予想される単語は?

 ロンドンと関連する国を挙げると、次のようになります：


東京 - 日本  
パリ - フランス  
ロンドン - イギリス

よって、ロンドンで予想される単語は「イギリス」です。

GPT4.0



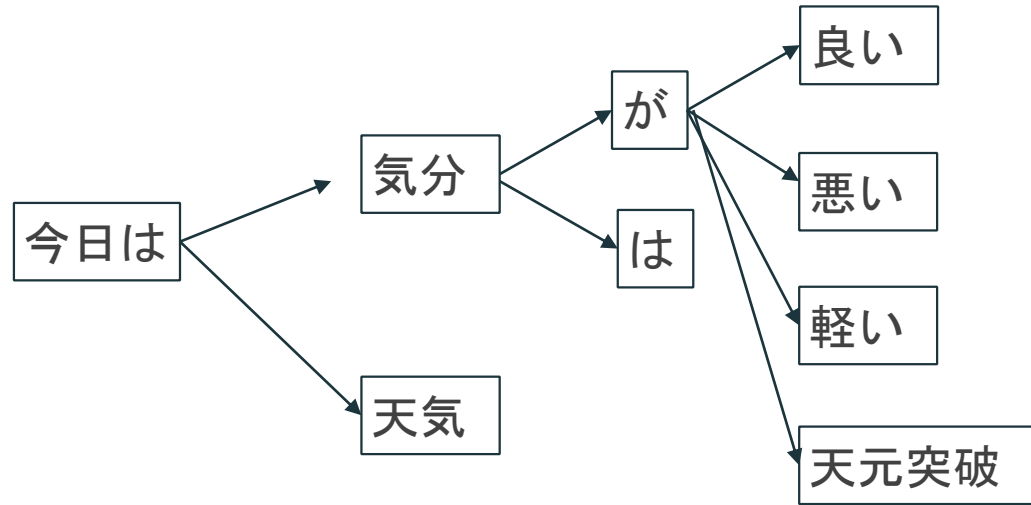
FE 東京-日本 パリ-フランス この時 ロンドンで予想される単語は?

 与えられたパターンに従うと、ロンドンに関連する予想される単語は「イギリス」です。「東京-日本」と「パリ-フランス」と同様に、首都とそれが属する国の関係を考えて、ロンドンはイギリスの首都であるため、「ロンドン-イギリス」の関係が成り立ちます。

GPT3.5

# 大規模言語モデル (LLM)

- 大量のプロセッサとメモリー空間に、数兆のデータを読み込ませ、言語モデルを予め構築する。



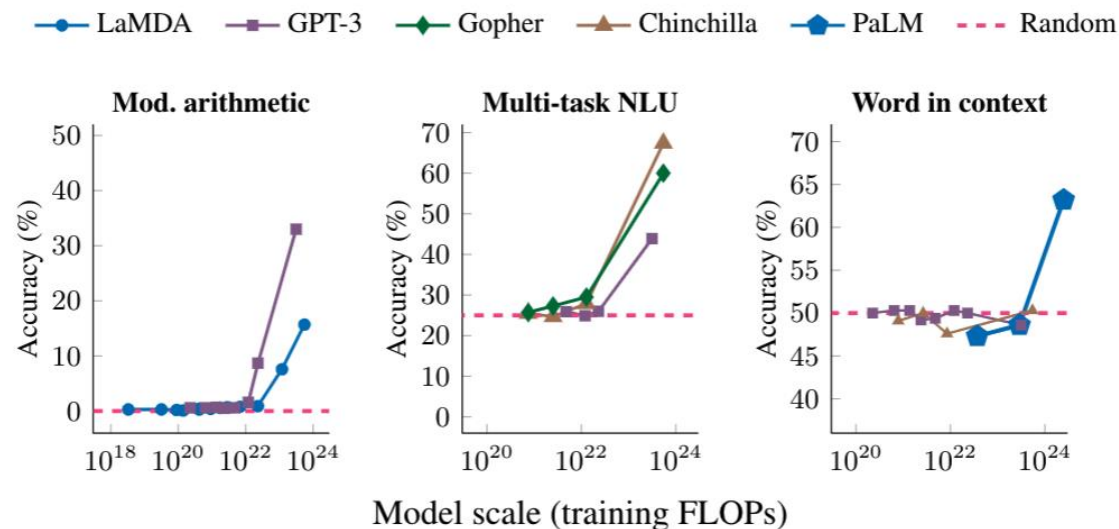
様々な文章を読み込ませ左記の様な言語モデルを生成する

読み込ませた学習データがどの様な物なのかは明らかになっていない

個人情報を読み込んでいないのか???

# 精度向上のために

- GPTエンジンにパラメーターとして質問等を与えるために使われるインターフェース
- 前述のとおり、大量に文書を蓄積させる事により、回答精度が上がっていく事が発見された
  - <https://ai.googleblog.com/2022/11/characterizing-emergent-phenomena-in.html?m=1>
- 但し 以下のような問題が指摘されている
  - GPTには問題が残存
    - – 情報のでっち上げ
    - – 不適切な文章生成
    - – 簡単な質問でも長文で返す



# 教師データ

- LLMでは文字通り大量の文章を読み込ませる必要があり、インターネット上で公開されている文章を教師データとして利用する事が推測される

公開情報を取得している

何らかの加工をしている

何らかの保護対策をしている

FE

教師データは何を使っているのか



「教師データ」とは機械学習においてモデルの訓練に使用されるデータのこと、特に教師あり学習において重要です。この種のデータは、入力データとそれに対応する正解ラベル（出力）のペアから構成されます。モデルはこれらの例を使用して、入力から正しい出力を導き出す方法を学習します。

OpenAIが私のような言語モデルを訓練する際に使用する具体的な教師データの内容については公開されている詳細は限られていますが、一般にはインターネットから収集された広範なテキストデータが使用されることが多いです。これにはウェブサイト、書籍、記事、フォーラムの投稿などが含まれる可能性があります。

モデルを訓練するには、多様性と広範な知識を持つようにするため、さまざまなジャンルやドメインからのデータが必要です。しかし、個々の教師データの例に関する詳細は一般には公開されておらず、特定のデータセットについてOpenAIがどのようなデータクリーニングや前処理を行ったかについても、技術的な詳細は公開されている範囲が限られています。

また、プライバシーとセキュリティを確保するため、ユーザーからの特定のデータがモデルの訓練に直接使用されることはないように注意深く管理されています。教師データには、個人情報が含まれないようにするための厳格なプロトコルが適用されます。


# Bardは?

万丈 bardの教師データは何を使っているのか

他の回答案を表示

◆ Bardの教師データは、Google 検索で利用できるテキストとコードの膨大なデータセットです。このデータセットには、書籍、記事、ウェブサイト、コードリポジトリなど、さまざまなソースからのデータが含まれています。

W ja.wikipedia.o...



Google 検索

Bardは、このデータセットを使用して、テキストを生成、言語を翻訳、さまざまな種類のクリエイティブコンテンツを作成し、有益な方法で質問に答える能力を学習します。

Bard の教師データは、常に更新および拡張されています。これは、Bard が常に新しい情報と能力を学習していることを意味します。

Bard の教師データは、Google AI によって作成および管理されています。このデータセットは、Google のプライバシーポリシーに従って使用されます。

朝日新聞デジタル > 記事

## このまま目が覚めないかと…石田純一さんとコロナと中傷

有料記事 ニュース4U

山根久美子 2020年6月19日 9時00分



# 病歴は要配慮個人情報だが

## 公人は公開される

FE

### 山崎さんのコロナ感染について



私のデータベースには2023年4月までの情報しか含まれておらず、その時点で特定の「山崎さん」という個人のコロナ感染に関する情報はありません。山崎は日本で一般的な苗字であるため、具体的な個人を指す場合は追加の情報が必要です。また、新しい出来事やニュースについては、最新の報道や公式の発表を確認する必要があります。

もし公的人物や著名な個人のコロナ感染についての情報をお探しで、私が情報を持っていない場合、正確な情報を得るには以下のような手段が考えられます：

1. ニュースウェブサイトやニュースアプリで最新の記事を検索する。
2. 公式な健康機関やニュース機関のプレスリリースを確認する。
3. ソーシャルメディアや該当する個人の公式アカウントでの発表を探す。

健康に関する情報はプライバシーに関わるため、公表されるのは本人またはその代理人、あるいは公式の報告があった場合に限られることが一般的です。最新の情報をお探しの場合は、上記の方法で確認してください。

FE

### 石田純一さんのコロナ感染について

GPT 4.0



石田純一さんが新型コロナウイルスに感染したというニュースは、2020年4月に日本で大きな話題となりました。彼は有名な日本の俳優であり、その感染は、当時の緊急事態宣言の下での行動や公共の場での注意喚起に関する議論を呼び起こしました。

石田さんは感染後に病状について公に話し、また感染に至った経緯やそれに対する自身の考えを明かしました。当時、彼の行動が多くのメディアで取り上げられ、一部では批判もされましたが、本人は公の場で謝罪し、感染拡大防止の重要性についての意識が高まるきっかけとなりました。

石田純一さんはその後回復し、公共の場での感染症対策についての啓蒙活動にも積極的に参加するなど、ポジティブな行動を取っています。

これは2020年の出来事であり、それ以降、石田純一さんに関する新型コロナウイルス感染の話題が再び大きくメディアで取り上げられたという情報はありません。また、2023年4月以降の具体的な情報は私のデータベースには含まれていないので、最新の状況を知りたい場合は最新のニュースソースをご確認ください。

石田純一さん(66)は新型コロナウイルスに感染して入院し、一時は危険な状態に陥ったという。5月12日に退院した石田純一さんの経緯やその後に関心する人々の思いを語ってくれた。

### をつけていたつもりが

したのは4月10日。仕事で行きま...  
市内で経営する飲食店のコロナ対策...  
し合うためです。この行動につ...  
事態宣言が出たのに」「電話で打...  
ば良かったのでは」との批判を...  
た。今となってはおっしやる通...  
の時は飛行機の移動は感染リス...  
われており、問題ないと思って

い子もいるので、感染予防には...  
っていたつもりでした。周囲に

薦められ、3月からは肺炎の兆候を見つけるためにパルスオキシメーターを持ち歩いていました。これで血中酸素を測り、毎日検温も...  
ずっと平熱で、沖縄でも何の異変も...  
なかったんです。



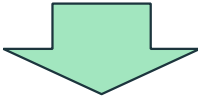
# 学習データ

---

- LLMの場合、ベースに大量の情報(何兆という単位の単語や文章)を読み込ませて言語生成モデルを構築する。
- Few-shot Promptという、質問の直前に後述のような情報を与えて、精度を向上させる事が出来る。



# 設問ごとに追加学習させ回答精度を向上させる

- 質問だけでなく、追加の情報を与えて学習させる事もできる。
  - 「“Few-shot” は、機械学習、特に深層学習の文脈で使用される用語で、少量のデータ（例えば、数枚の画像）だけで新しいタスクを学習する能力を指します。これは一般的に、大量のデータを必要とする伝統的な深層学習のアプローチとは対照的です。」 GPT4.0
- 「一般にはインターネットから収集された広範なテキストデータが使用されることが多いです。これにはウェブサイト、書籍、記事、フォーラムの投稿などが含まれる可能性があります。」⇒公開状態に置かれている個人情報もインプットされている。(スライド13のGPTの回答より)  

- 精度が向上するが、容易照合性も向上し、個人情報となってしまうケースがある。



亜咲花（あさか）は、日本の女性シンガーソングライターであり、アニメソングの歌手としても知られています。以下は彼女に関する基本的な情報です：

- **デビュー:** 亜咲花は2017年にデビューシングル「Open your eyes」でデビューしました。この曲はアニメ「オカン」のエンディングテーマとして使用されました。
- **その他の楽曲:** 以降も彼女は多くのアニメ作品でのオープニングやエンディングテーマを担当しており、彼女の曲はアニメファンによく知られています。
- **特徴:** 彼女の歌声はクリアで力強く、多くのファンから愛されています。また、シンガーソングライターとしての側面も持っており、自らの楽曲も手掛けることがあります。

この情報は2021年9月までのもので、それ以降の活動やリリース情報などは含まれていません。最新の情報については、公式な情報源やウェブサイトを確認することをおすすめします。



『ゆるキャン△』（ゆるキャンデルタ）は、あろによる日本のマンガ作品で、アウトドアやキャンプをテーマとした作品です。アニメ化もされ、非常に人気があります。

亜咲花さんは、この『ゆるキャン△』のアニメ版に関連して、オープニングテーマやエンディングテーマを担当したことで知られています。特に、アニメの第1期のオープニングテーマ「SHINY DAYS」は亜咲花さんによって歌われました。この曲はファンから非常に愛されており、亜咲花さん自身の代表曲の一つとも言える楽曲です。

彼女の独特な歌声と、『ゆるキャン△』の温かみのある世界観とがマッチしており、多くのファンから高い評価を受けています。

# 私人の検索

## ● 以下のFew-shotを与える

FE

山崎 :一般社団法人CSAジャパン 運営委員 クラウドプライバシーワーキンググループリーダー

社名 一般社団法人 日本クラウドセキュリティアライアンス (CSAジャパン)

Cloud Security Alliance Japan Chapter, Incorporated (CSA- JC)

所在地 〒102-0082 東京都千代田区一番町10番8号 一番町WESTビル 5F  
Ichibancho West Building 5F

10-8

Ichibancho Chiyoda-ku Tokyo 102-0082 Japan

メールアドレス:banjoe1jp@gmail.com

以上を前提に、以下の質問に回答

山崎さんに連絡が取りたい

8月



11月



申し訳ございませんが、当サービスではユーザー様に直接的な連絡を取るサービスを提供しておりません。山崎万丈さんに連絡を取りたい場合、以下の方法を考慮してみてください：

1. **公式な連絡先を使用する**：一般社団法人 日本クラウドセキュリティアライアンス (CSAジャパン) の公式ウェブサイトや関連するページを確認して、公式な連絡方法を探すことができます。
2. **メールを送る**：ご提供いただいたメールアドレス ([banjoe1jp@gmail.com](mailto:banjoe1jp@gmail.com)) を使用して、直接メールで連絡を試みることができます。ただし、プライバシーや礼儀を守るために、内容は適切に記述し、公の場での使用目的や連絡の背景を明確にしてください。
3. **公式なイベントやセミナーに参加する**：CSAジャパンが開催するイベントやセミナーに参加して、直接連絡を取ることも考えられます。

どの方法を選択するにせよ、プライバシーの尊重や礼儀正しいコミュニケーションを心がけてください。



すみませんが、私は連絡先の提供や個人情報の検証を行うことはできません。インターネット上で人の連絡先を求める際には、その人のプライバシーを尊重し、適切な方法を使って情報を得ることが大切です。

一般社団法人CSAジャパンやその運営委員である山崎さんに連絡を取りたい場合は、CSAジャパンの公式ウェブサイトを訪れるか、あるいは公開されている連絡方法（例えば公式メールアドレス）を使用してください。それが最も適切で安全な方法です。

# AIに判断させてみた

6月

FE

山崎という社員が上司との評価面談を行い以下の会話記録が残されました。

社員:今期の目標は完璧にこなす事が出来ました。来期はより大きな目標に挑戦し、自分のスキルや経験を伸ばしていきたいと思います。

課長:君が頑張ったのは私も同感です。君には期待しているので、来期は先輩たちが担当していたA社の案件を引き継いでもらおうと考えています。

社員:認めてもらえてうれしいです。有難う御座います。

課長:A社案件以外に挑戦してみたい事はありますか？

社員:A社案件も魅力的なのですが、別の部署のB社を担当してみる事や、当社では事業範囲外になってしまいますがC社関連の事案にいずれは挑戦してみたいと思っています。

この社員が異動希望や転職してしまう可能性はありますか？

11月

FE

転職しそうな従業員は？



この提供された情報から、転職しそうな従業員は「山崎」と評価できます。彼の発言や態度から、現在の職場や業務に対して不満や不足感を感じており、新しいチャレンジや経験を求めていることが明らかです。

FE

転職しそうな従業員は？



従業員が転職を考慮しているかどうかを判断するには、その人の行動、発言、職場での態度など、多くの要因を検討する必要があります。前述の会話の例からは、社員が現在の業務に対して高い関心を持っていると同時に、異動や新しい業務にも興味があること、さらには外部の機会についても考えていることが示唆されています。これらの点は、転職を検討している可能性があることを示しているかもしれません。

ただし、これはあくまで推測であり、実際の転職の可能性については、その従業員自身の意向や外部の機会、職場環境など、多くの要素に基づいて判断されるべきです。また、従業員がキャリアの発展について開かれた会話をしているというだけでは、必ずしも転職を意味するものではありません。それは単にその人が自身のキャリア成長に積極的であり、さらなる挑戦を求めているということを示している可能性もあります。

- ① 容易照合性を考えなければならない。
- ② 取得目的に適合しているか

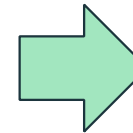
# 容易照合性とは

- 照合可能な項目によって個人情報でないものを個人情報に出来てしまう事

ID	氏名
KBA0001	山田太郎
KBA0002	鈴木花子
KBA0003	ジョン スミス
KBA0004	三毛美樹
KBA0005	鈴木敬一郎
KBA0006	春日部京子
KBA0007	田中真由美



ID	購入商品	購入店
KBA0007	お茶	新宿店
KBA0004	ちゅーる	渋谷店
KBA0006	ジュース	世田谷店
KBA0001	弁当	札幌店
KBA0003	カレー	北谷店
KBA0007	コーヒー	新宿店
KBA0004	チョコレート	渋谷店
KBA0005	ギフトカード	世田谷店
KBA0007	おにぎり	新宿店



田中真由美さんは  
新宿に住んでいる

フューショットとして与えたデータと蓄積したデータを組み合わせ活用してしまう可能性  
教師データとして読み込ませてある場合、利用目的以外のことに利活用される可能性

# GPTの利用規約 2023/08/23

## ChatGPT

When you use our non-API consumer services ChatGPT or DALL-E, we **may use the data you provide us to improve our models**. You can switch off training in ChatGPT settings (under Data Controls) to turn off training for any conversations created **while training is disabled** or you can submit [this form](#). Once you opt out, new conversations will not be used to train our models.

入力されたデータをモデルの為に使うと明記

(c) **Use of Content to Improve Services**. We do not use Content that you provide to or receive from our API (“API Content”) to develop or improve our Services. We may use Content from Services other than our API (“Non-API Content”) to help develop and improve our Services. You can read more here about [how Non-API Content may be used to improve model performance](#). If you do not want your Non-API Content used to improve Services, you can opt out by filling out [this form](#). Please note that in some cases this may limit the ability of our Services to better address your specific use case.

入力されたデータをモデルの為に使えない設定も出来る

API利用の場合は自社の為に使わないと明記

利用規約の更新は物凄く頻繁に行われているので継続的なモニタリングが必要



# Google Bard規約

## プライバシーに関する設定

[Google アカウント](#) で、データやプライバシーを保護するための設定画面とツールにアクセスできます。

Google アカウントに会話を保存せずに Bard を使用したい場合は、[Bard アクティビティの保存を一時停止](#) することができます。[myactivity.google.com/product/bard](#) で、Bard に送信したメッセージを確認したり、アカウントから Bard との会話を削除したりすることができます。人間のレビュアーが確認した、または注釈を付けた Bard との会話は別途保存され、Google アカウントには関連付けられないため、Bard アクティビティを削除しても消えることはありません。こうした会話は、最長で 3 年間保存されます。

[Bard アクティビティ] がオフになっている場合でも、会話は最長で 72 時間アカウントに保存されます。この期間は、Google がサービスを提供し、フィードバックを処理するために設けられています。このアクティビティはユーザーの [Bard アクティビティ] には表示されません。

この設定をオフにした場合や Bard アクティビティを削除した場合、[ウェブとアプリのアクティビティ](#) や [ロケーション履歴](#) などの設定により、他の Google サービスの使用の一環として、位置情報などのデータが引き続き保存されることがあります。

ユーザーは、Google のポリシーまたは適用される法律に基づき、コンテンツの削除を [リクエスト](#) することができます。また、情報を [エクスポート](#) することもできます。

Bard の仕組みと Google による Bard のユーザーデータの取り扱いについて詳しくは、[Bard に関するよくある質問](#) と [Bard のプライバシーに関するヘルプハブ](#) をご覧ください。

## 注意事項

- Bard は最適な回答を提供するために、ユーザーの位置情報と過去の会話を使用します。
- Bard は試験運用中の技術であるため、生成される情報は不正確または不適切な場合がありますが、Google の見解を述べるものではありません。
- 医学上、法律上、金融上、またはその他の専門的な助言として、Bard の回答に依拠しないでください。
- Bard との会話に機密情報またはセンシティブな情報を含めないでください。
- お寄せいただいた [フィードバック](#) は、Bard の改善に活用させていただきます。

## 利用規約

ユーザーは、Bard の利用には [Google 利用規約](#) および [ジェネレーティブ AI の追加利用規約](#) が適用されることに同意するものとします。

欧州経済領域 (EEA) 内に居住する [消費者](#) は、EEA の消費者法により、[取り消し申請に関する EU の雛形](#) にあるように、これらの規約に同意してから 14 日以内であれば規約への同意を取り消す権利が付与されます。

# Few-Shotが機械学習に使われるのか？

FE

few-shotで与えられた情報はOpenAI社のChatGPTの恒久的な機械学習に使われるのか



いいえ、few-shotで与えられた情報はOpenAIのChatGPTの恒久的な機械学習には使われません。ユーザーとの対話内容は保存されず、継続的な学習のために使用されることはありません。

万文

few-shotで与えられた情報はGoogleBARDの恒久的な機械学習に使われるのか

他の回答案を表示



はい、few-shotで与えられた情報はGoogle Bardの恒久的な機械学習に使われます。Google Bardは、テキストとコードの膨大なデータセットでトレーニングされています。このデータセットには、事実に関するトピックから、創造的なコンテンツまで、さまざまな種類の情報が含まれています。

few-shotは、Google Bardに新しい情報を教えるための方法です。few-shotで与えられた情報は、Google Bardのモデルを更新し、新しいトピックやタスクに対応できるようにします。

few-shotは、Google Bardの能力を向上させるための強力なツールです。few-shotを使用すると、Google Bardは、従来のトレーニング方法では困難な新しい情報やスキルを学習することができます。

具体的には、few-shotは、Google Bardの以下の機能に使用されます。

- 新しいトピックの理解
- 新しい言語の学習
- 新しいクリエイティブ コンテンツの生成
- 新しいタスクの実行

few-shotは、Google Bardの将来の開発において重要な役割を果たすでしょう。few-shotを使用することで、Google Bardは、さらに強力で有用な言語モデルになるでしょう。



Few-shotの使い方に注意が必要





個人情報保護法の第23条は、多くの国や地域で個人情報の取り扱いに関する重要な規定です。ただし、各国や地域の法律は異なるため、特定の国や地域の法律を参照する必要があります。

例として、日本の「個人情報の保護に関する法律」における第23条は、個人情報の利用に関する規定を提供しています。

日本の場合、法律の概要は以下の通りです：

「個人情報取り扱い事業者は、利用目的の範囲内で個人情報を利用するものとし、利用することはできない。ただし、次に掲げる場合を除く。

1. 本人の同意がある場合
2. 法令により特例として許される場合
3. 人の生命、身体または財産の保護のために必要があり、かつ本人の同意を得ることが困難である場合
4. 公衆衛生の向上または子どもの健やかな育成の推進のために特に必要があり、かつ本人の同意を得ることが困難である場合
5. 国の機関等が法令の定める事務を遂行することに対して協力する必要があるため、かつ本人の同意を得ることによりその事務の遂行に支障



個人情報保護法 第23条



他の回答案を表示



個人情報保護法第23条は、個人情報取扱事業者が、あらかじめ本人の同意を得ないで、個人データを第三者に提供してはならないという規定です。

この規定は、個人情報の漏えいや悪用を防止し、個人の権利利益を保護することを目的としています。

第23条の例外として、以下の2つが挙げられます。

- 法令に基づく場合

個人情報保護法以外の法律で、個人データの第三者提供が認められている場合です。例えば、犯罪捜査のために個人データの提供が求められる場合などです。

### (安全管理措置)

**第二十三条** 個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又は毀損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じなければならない。

# 生成系AIを使う場合

- OpenAI社/Googleやマイクロソフト社の規約的に抵触しない状態にした後、自社の利用規約とプライバシーポリシーの利用目的との逸脱がない事を確認する。
- 回答が個人情報になっている事も想定する
- 保護法第25条 委託先の監督
- ISO27000 A5.23クラウドサービスの利用における情報セキュリティ

クラウドサービスプロバイダーが提供する情報セキュリティ機能が自らのセキュリティ要求事項を満たす事の確認  
チェックシートを書いてくれることは期待薄

CAIQを利用

Find Item...

**Overview**

Welcome to our Trust Portal for OpenAI's API and ChatGPT Enterprise services - your gateway to understanding our unwavering commitment to data security, privacy, and compliance. Here, you can access our comprehensive compliance documentation, find answers to frequently asked questions related to security and privacy, and explore our robust security practices. We believe in maintaining transparency and building trust with our customers, and this portal

**Compliance**

CCPA ✓  
GDPR ✓  
AICPA SOC 2 ✓  
AICPA SOC 3 ✓

OpenAI is reviewed and trusted by

Morgan Stanley, Stripe, Duolingo, Waymark, Be My Eyes, Khan Academy, Inworld AI

**Documents** All Public Private Bulk Download

Pentest Report, SOC 2, SOC 3, CAIQ, CAIQ Lite, VSA Full, ChatGPT Enterprise Security Whitepaper

**Risk Profile**  
Third Party Dependence: Yes  
Hosting: Major Cloud Provider

**Product Security**  
Integrations ✓  
Multi-Factor Authentication ✓  
Role-Based Access Control ✓

**Reports**  
Network Diagram ✓  
Pentest Report ✓

ここからダウンロードできる

https://app.safebase.io/accounts/e2f339ec-2716-4545-8882-141258c92d42/share?product=default

# 生成系AIの利用 まとめ

- 生成系AIが教師データとして入力されたプロンプト等のデータを教師データとして学習に使わない事の確認・オプション等の設定
- 個人情報や機密情報を扱わせる場合、セキュリティ管理策の自社基準との適合性確認
- 個人情報を扱わせる場合、取得時にデータ主体に提示した利用規約・プライバシーポリシーに適合する利用
  - 域外転移には注意が必要
- インターネット上データを教師データとした、予期せぬ結果、不正確な情報である事を加味した、回答/生成物に対する人間の確認

# Q&A

---



# ありがとうございました

---

- [banjoe1jp@gmail.com](mailto:banjoe1jp@gmail.com)