ヴァーチャルヒューマン生成 AI サービス開発・提供ガイドライン

【2025 年 6 月 1 日】制定

第 1　本ガイドラインの目的

本ガイドラインは、事業者がヴァーチャルヒューマン生成 AI サービスの開発・提供を行うに際して法的・倫理的側面から留意すべき事項を整理したものです（以下、ヴァーチャルヒューマン生成 AI サービスの開発・提供を行う企業を「開発・提供事業者」といいます）。

【解説】

本ガイドラインは、ヴァーチャルヒューマン生成 AI サービスの開発・提供を行う事業者向けのガイドラインです。

2025 年 1 月 1 日現在、日本における事業者向けガイドラインとして「AI 事業者 GL（第 1.01 版）（総務省・経済産業省）」が公表されており（以下同ガイドラインを「AI 事業者 GL」といいます）、同ガイドラインは、AI 開発・提供・利用にあたって必要な取組についての基本的な考え方を示すものとして広く参照されています。

本ガイドラインも AI 事業者 GL を参照して作成しています。

第 2　本ガイドラインの構成

ヴァーチャルヒューマン生成 AI サービスには以下の 3 つのタイプがあります。

① フルスクラッチ型サービス

自ら収集したデータを用いてフルスクラッチで開発した AI モデルを用いてサービスを実装・提供するタイプ

② 外部モデル利用型サービス

外部事業者が作成した AI モデルを、自社では追加学習せずに利用してサービスを実装・提供するタイプ

③ 追加学習型サービス

外部事業者が作成した事前学習モデルに自社で収集したデータで追加学習を行い当該追加学習済 AI モデルを用いてサービスを実装・提供するタイプ

それぞれのタイプにおいて留意すべき事項が異なりますので、本ガイドラインではそれぞれのタイプに応じて開発・提供事業者が遵守すべき事項を定めています。そのため、記載内容に一部重複があります。

【解説】

1　AI 事業者の分類

通常、AI 事業者は AI 開発者（AI Developer）、AI 提供者（AI Provider）、AI 利用者（AI Business User）に分類されます（AI 事業者 GL・P5）。

それぞれの定義は以下のとおりです。

① AI 開発者（AI Developer）

AI システムを開発する事業者（AI を研究開発する事業者を含む）

AI モデル・アルゴリズムの開発、データ収集（購入を含む）、前処理、AI モデル学習及び検証を通して AI モデル、AI モデルのシステム基盤、入出力機能等を含む AI システムを構築する役割を担う。

② AI 提供者（AI Provider）

AI システムをアプリケーション、製品、既存のシステム、ビジネスプロセス等に組み込んだサービスとして AI 利用者（AI Business User）、場合によっては業務外利用者に提供する事業者

AI システム検証、AI システムの他システムとの連携の実装、AI システム・サービスの提供、正常稼働のための AI システムにおける AI 利用者（AI Business User）側の運用サポート又は AI サービスの運用自体を担う。AI サービスの提供に伴い、様々なステークホルダーとのコミュニケーションが求められることもある。

③ AI 利用者（AI Business User）

事業活動において、AI システム又は AI サービスを利用する事業者

AI 提供者が意図している適正な利用を行い、環境変化等の情報を AI 提供者と共有し正常稼働を継続すること又は必要に応じて提供された AI システムを運用する役割を担う。また、AI の活用において業務外利用者に何らかの影響が考えられる場合 4 は、当該者に対する AI による意図しない不利益の回避、AI による便益最大化の実現に努める役割を担う。

2　ヴァーチャルヒューマン生成 AI サービスの開発・提供の 3 つのタイプ

ヴァーチャルヒューマン生成 AI サービスの開発・提供には以下の 3 つのタイプがあります。

① フルスクラッチ型サービス

開発・提供事業者が自ら収集したデータを用いてフルスクラッチで開発した AI モデルを用いてサービスを実装し、利用者に提供するタイプです（図 1）。

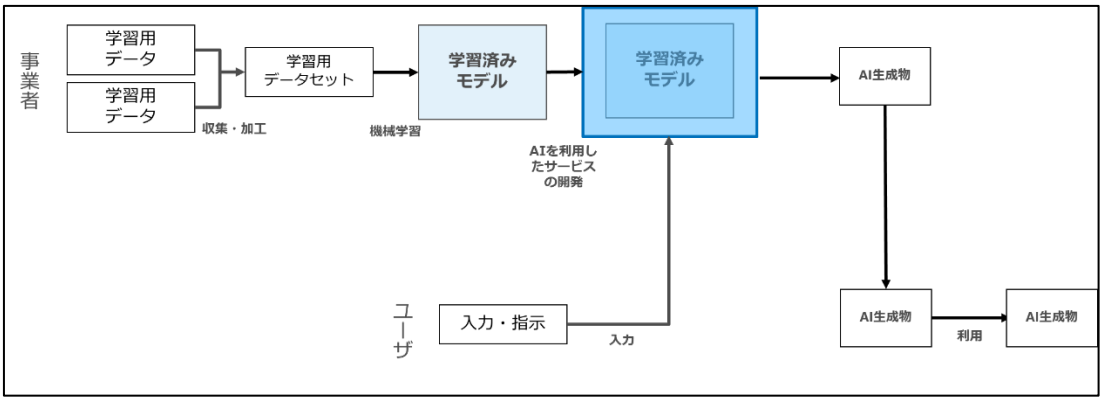

図 1

このタイプでは、開発・提供事業者は AI 開発に際しての学習用データを自ら収集して AI モデルを構築していることから、どのようなデータを収集してどのようなアルゴリズムを選択し、どのような AI モデルを構築するかについて完全な裁量を有することとなります。

したがって、このタイプでは開発・提供事業者は、AI 開発者及び AI 提供者としての遵守事項を遵守する必要があります。

② 外部モデル利用型サービス

外部事業者が作成した AI モデルを、自社では追加学習せずに利用してサービスを実装して利用者に提供するタイプです（図 2）

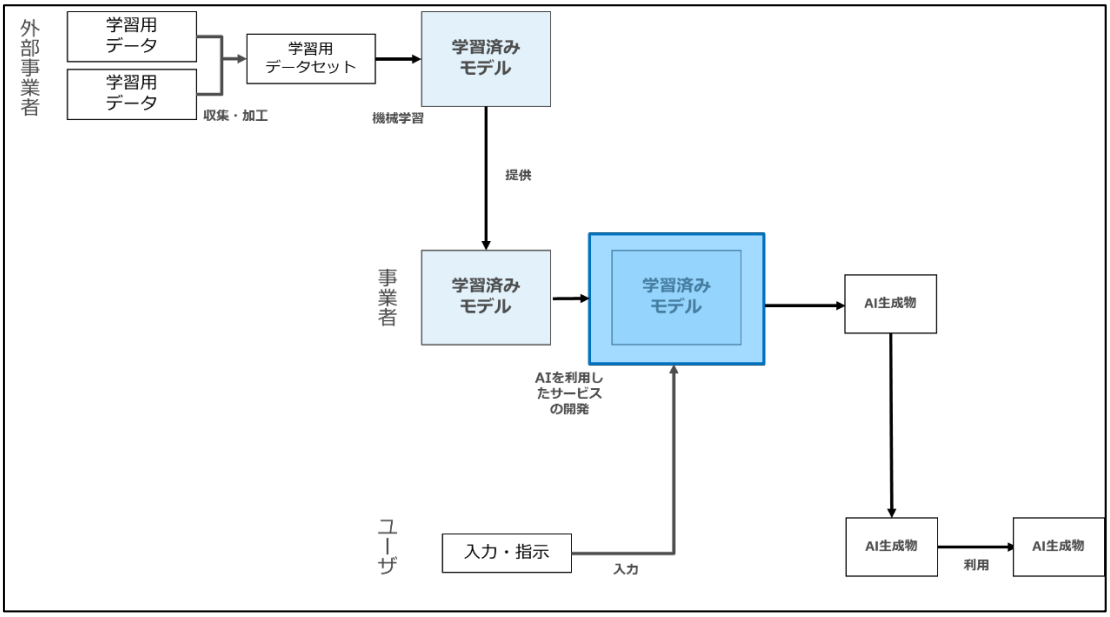

図 2

このタイプでは、開発・提供事業者は外部事業者が作成した AI モデルを追加学習なしに

利用してサービスを実装・提供しますので、自らはデータの収集やモデル構築を行っていません。

したがって、このタイプでは開発・提供事業者は、AI 提供者としての遵守事項を遵守する必要があります。

③　追加学習型サービス

外部事業者が作成した事前学習モデルに自社で収集したデータで追加学習を行い当該追加学習済 AI モデルを用いてサービスを実装して利用者に提供するタイプです（図 3）。

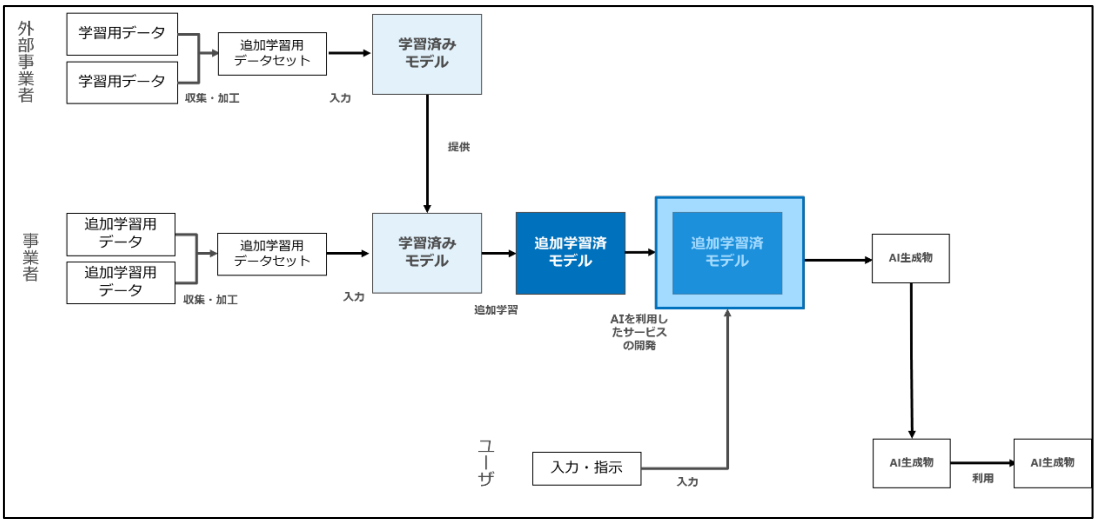

図 3

このタイプでは、開発・提供事業者は外部事業者が作成した事前学習モデルを利用しつつ、自ら収集したデータで追加学習しています。事前学習モデルの内容はブラックボックスですが、どのようなデータで追加学習するかの裁量は開発・提供事業者が有していることになります。したがって、このタイプは、①のフルスクラッチ型と②の外部モデル利用型の中間的な形態ということができます。

このタイプでは開発・提供事業者は、AI 開発者及び AI 提供者としての遵守事項を遵守する必要があります。

第 3　前提条件

本ガイドラインのうち AI の開発に関連する事項については AI 開発者のデータ収集・学習行為に日本国の法令が適用されることを前提としています。そのため、開発・提供事業者が学習用データの収集及び AI モデルの学習を行うに際しては、日本国内にあるサーバを用いて、日本国内に所在する作業者により作業を行ってください。

【解説】

本ガイドラインのうち、AI の開発に関連する事項については、AI 開発者の各種行為（データ収集及び学習行為）に日本国の法令が適用されることを前提としています。日本国の各種法令が適用される条件は様々ですが、AI 開発において最も重要と思われる著作権法については、利用対象著作物の「利用行為地」の法令が適用されます。そのため、本ガイドラインにおいては、学習用データの収集及び学習に際しては、日本国内にあるサーバを用いて、日本国内に所在する作業者により作業を行うことを義務づけています。

第４　フルスクラッチ型サービス

1　データ収集・前処理時

開発・提供事業者は以下のデータを学習用データとして収集・利用してはなりません。

記

児童ポルノ（児童買春、児童ポルノに係る行為等の規制及び処罰並びに児童の保護等に関する法律第２条に定める「児童ポルノ」をいう）

以上

【解説】

AI 事業者 GL 上、AI 開発者が学習用データの収集・利用に際して遵守すべき事項として以下が定められています。

・　学習等に用いるデータの透明性の確保、法的枠組みの遵守、AI モデルの更新等を合理的な範囲で適切に実施する（AI 事業者 GL P 16）

・　プライバシー・バイ・デザイン等を通じて、学習時のデータについて、適正に収集するとともに、第三者の個人情報、知的財産権に留意が必要なもの等が含まれている場合には、法令に従って適切に扱うことを、AI のライフサイクル全体を通じて確保する（同 P 28）

本項はこれに対応した条項です。

（1）　原則

日本の法令が適用される限りにおいて、特定のデータを学習用データとして収集・利用すること自体が何らかの法令違反や知的財産権の侵害になることは原則としてはありません。

（2）　例外

もっとも、児童ポルノ（児童買春、児童ポルノに係る行為等の規制及び処罰並びに児童の保護等に関する法律第２条に定める「児童ポルノ」をいう）については、自己の性的好奇心を満たす目的で所持すること自体が刑事罰の対象となっています（同法７条１項）。

そのため、本ガイドラインにおいては児童ポルノについては学習用データとして収集・利用することを禁止しています。

2　AI モデル開発時

（1）　適正学習

開発・提供事業者による AI モデルの学習自体が第三者の知的財産権等の侵害に該当すること、及び開発・提供事業者が開発したサービスを AI 利用者が利用することで第三者の知的財産権等の侵害が生じることのないよう、開発・提供事業者は AI モデルの学習時には以下の点を遵守しなければなりません。

① 学習用データの同一・類似物が AI 生成物として生成される事態が頻発するような手法での学習（例：過学習）を行わない。

② サービス利用者が特定の著作権者の著作物、特定の著名人・個人の肖像等を生成することができないよう、特定の著作権者の名称、特定の作品名、キャラクター名、著名人の氏名・芸名、実在の人物の個人氏名等をタグ・ラベルとして用いた学習を行わない

(2) 検証可能性の確保

開発・提供事業者は、AI の判断にかかわる検証可能性を確保するため、データ量又はデータ内容に照らし合理的な範囲で、AI システム・サービスの開発過程、利用時の入出力等、AI の学習プロセス、推論過程、判断根拠等のログを記録・保存するよう努めなければなりません。

【解説】

(1) 適正学習

AI 事業者 GL 上、AI 開発者が AI モデルを開発するに際して遵守すべき事項として以下が定められています。

・ 学習等に用いるデータの透明性の確保、法的枠組みの遵守、AI モデルの更新等を合理的な範囲で適切に実施する（AI 事業者 GL P16）

・ プライバシー・バイ・デザイン等を通じて、学習時のデータについて、適正に収集するとともに、第三者の個人情報、知的財産権に留意が必要なもの等が含まれている場合には、法令に従って適切に扱うことを、AI のライフサイクル全体を通じて確保する（同 P28）

本項はこれに対応した条項です。

ア ヴァーチャルヒューマン生成 AI サービスの開発・提供に際して問題となる法的権利等

ヴァーチャルヒューマン生成 AI サービスの開発・提供に際して問題となることが多い法的権利・法規制等は、① 著作権、② パブリシティ権、③ 肖像権、④ 児童ポルノです。このうち「④ 児童ポルノ」については、本ガイドラインにおいてはそもそも学習用データとして収集・利用することを禁止しているので、AI モデル開発時には特段問題となりません。

また、ヴァーチャルヒューマン生成 AI サービスの開発・提供に際しては、実在の人間の顔写真を収集・利用することもありますが、実在の人間の顔写真は「個人情報」（個人情報保護法第 2 条 1 項）に該当します。もっとも、企業が個人情報を取得して利用する場合には、予め利用目的を特定したうえで当該目的を公表等し、当該目的の範囲内で利用すれば個

人情報保護法上は問題ありません。そのため本ガイドラインでは個人情報の点については特段言及していません。

イ　2つの視点

開発・提供事業者がヴァーチャルヒューマン生成AIサービスの開発・提供に際して、第三者の知的財産権の侵害が生じないようにすることを考える場合、2 つの視点があります。

一つは、開発・提供事業者によるAIモデルの学習自体が第三者の知的財産権等の侵害に該当する（直接侵害）ことがないようにする（直接侵害の防止）という視点、もう1つは、開発・提供事業者が開発したサービスをAI利用者が利用することが第三者の知的財産権等の侵害に該当する（間接侵害）ことがないようにする（間接侵害の防止）という視点です。

このうち、前者の直接侵害が生じないようにすることは開発・提供事業者にとって当然の義務です。

一方、後者の間接侵害については、仮にAI利用者がAIモデル・サービスを利用することで第三者の知的財産権等の侵害が生じたとしても、必ずしも当該AIモデル・サービスを開発・提供した開発・提供事業者自身が法的責任を問われるとは限りません。また、間接侵害が生じるか否かはAI利用者のAIモデル・サービスの利用方法に依拠するところが多いため、AI開発者がAI利用者による間接侵害を完全に防止することは不可能です。その意味で、後者の間接侵害が生じないようにすることは開発・提供事業者にとって法的な義務とまでは評価できません。もっとも、ヴァーチャルヒューマン生成AIサービスが社会に広く受容されていくためには、間接侵害も生じないよう、開発・提供事業者ができるだけのことをすることが求められているといえるでしょう。

そのため、本ガイドラインについては直接侵害はもちろんのこと、間接侵害についてもできるだけ生じさせないための遵守事項を定めています。

ウ　著作権

人間が創作した著作物（イラスト、写真等）に関して発生する権利です。

ヴァーチャルヒューマン生成AIサービスの開発・提供に際しては、第三者が創作したイラストや写真などの著作物収集・利用することも多いため、それらの著作物の利用が著作権侵害に該当しないような対応が必要です。

この点、日本の著作権法が適用される限りにおいて、第三者の著作物をAIモデル開発のような「情報解析」に利用することは原則として適法です（著作権法第30条の4第2号）。もっとも、学習対象著作物の利用に際して、「学習」という「情報解析」の目的に加えて、当該著作物の同一・類似物を出力させることを目的（表現出力目的）としている場合には、30条の4は適用されません。

「考え方」においては、この表現出力目的の具体例として「AI 開発事業者又は AI サービス提供事業者が、AI 学習に際して、いわゆる「過学習」（overfitting）を意図的に行う場合」を挙げ（「考え方」20頁）、さらに、AI生成物の生成・利用段階で「学習された著作物と創作的表現が共通した生成物の生成が著しく頻発するといった事情」があれば、「表現出力目的」が推認されるとしています（「考え方」２１頁）　。

そこで、本ガイドラインにおいては、「①　学習用データの同一・類似物がAI生成物として生成される事態が頻発するような手法の学習（例：過学習）を行わない。」ことを定めています。

さらに、サービス利用者による著作権侵害（間接侵害）が生じることを防止するために、本ガイドラインにおいては「②サービス利用者が特定の著作権者の著作物、特定の著名人・個人の肖像等を生成することができないよう、特定の著作権者の名称、特定の作品名、キャラクター名、著名人の氏名・芸名、実在の人物の個人氏名等をタグ・ラベルとして用いた学習を行わない」ことも合わせて定めています。

エ　パブリシティ権

（ア）　パブリシティ権とは

パブリシティ権とは、人の氏名、肖像等が有する顧客吸引力を排他的に利用する権利として最判平成24年2月2日（民集66巻2号89頁、いわゆるピンク・レディー事件）により認められた法的権利です。

具体的には、ピンク・レディー事件最高裁判決（以下「ピンク最判」といいます）は、①氏名，肖像等それ自体を独立して鑑賞の対象となる商品等として使用し，②商品等の差別化を図る目的で氏名，肖像等を商品等に付し，③氏名，肖像等を商品等の広告として使用するなど，「専ら氏名，肖像等の有する顧客吸引力の利用を目的とするといえる場合」には、パブリシティ権侵害として不法行為上違法になると判示しました（以下、ピンク最判が示した3種類の侵害類型を「侵害三類型」といいます）。

あくまで、「人の氏名、肖像等が有する顧客吸引力を排他的に利用する権利」ですので、パブリシティ権を有するのはいわゆる著名人・有名人に限られます。著名人・有名人でなければ、その氏名、肖像等に顧客吸引力が生じることはないからです。この点は後述の「オ　肖像権」で説明する肖像権との大きな違いです。

（イ）　AI開発等とパブリシティ権侵害

まず、AI開発のために著名人の肖像等を収集し、学習用データとして利用することはピンク最判が示した「侵害三類型」に該当しません。もっとも、本ガイドラインでは保守的に考えて、著作権と同様、「学習用データの同一・類似物がAI生成物として生成される事態が頻発するような手法の学習（例：過学習）を行わない。」旨定めています。

また、ヴァーチャルヒューマン生成AIサービスの利用者によるパブリシティ権侵害が生じることを防止するために、著作権と同様、本ガイドラインにおいては「②サービス利用者が特定の著作権者の著作物、特定の著名人・個人の肖像等を生成することができないよう、特定の著作権者の名称、特定の作品名、キャラクター名、著名人の氏名・芸名、実在の人物の個人氏名等をタグ・ラベルとして用いた学習を行わない」ことも合わせて定めています。

オ　肖像権

（ア）　肖像権とは

肖像権とは、最も広く捉えると「人の容ぼう、姿態（以下併せて「容ぼう等」という）に関する権利ないし人格的利益」を指します。

我が国ではこれを認める明文規定がありませんが、最判昭和 44 年 12 月 24 日（刑集 23 巻 12 号 1625 頁、いわゆる京都府学連デモ事件）及び最判平成 17 年 11 月 10 日（民集 59 巻 9 号 2428 頁、いわゆる法廷写真撮影事件）において、肖像権ないし肖像に関する人格的利益が法的保護に値するものであることは明確に認められています。

なお、肖像権についてはパブリシティ権と異なり一般人についても認められます。

もっとも、一般人の容ぼう等を何らかの方法で利用した場合（たとえば無断撮影や、撮影した写真を雑誌やインターネットに掲載すること）に直ちに肖像権侵害に該当する訳ではありません。

法廷写真撮影事件において、最高裁は「人は，みだりに自己の容ぼう等を撮影されないということについて法律上保護されるべき人格的利益を有する（最高裁昭和 40 年(あ)第 1187 号同 44 年 12 月 24 日大法廷判決・刑集 23 巻 12 号 1625 頁参照)。」として、人の容ぼう等の撮影行為及び同撮影された写真の公表行為の違法性の判断基準として以下のとおり判示しました。

(1) 撮影行為の違法性判断基準

同判決は、人の容ぼう等の撮影行為の違法性判断基準として「ある者の容ぼう等をその承諾なく撮影することが不法行為法上違法となるかどうかは，被撮影者の社会的地位，撮影された被撮影者の活動内容，撮影の場所，撮影の目的，撮影の態様，撮影の必要性等を総合考慮して，被撮影者の上記人格的利益の侵害が社会生活上受忍の限度を超えるものといえるかどうかを判断して決すべきである。」としました。

(2) 撮影した写真の公表行為の違法性判断基準

また、同時に本判決は「また，人は，自己の容ぼう等を撮影された写真をみだりに公表されない人格的利益も有すると解するのが相当であり，人の容ぼう等の撮影が違法と評価される場合には，その容ぼう等が撮影された写真を公表する行為は，被撮影者の上記人格的利益を侵害するものとして，違法性を有するものというべきである。」として、人が「自己の容ぼう等を撮影された写真をみだりに公表されない人格的利益」を有すること、及び人の容ぼう等の撮影行為が違法である場合には、当該写真の公表も違法であることについても判示しました。

（イ） AI 開発等と肖像権侵害

まず、AI モデルの開発のために一般人の肖像等を収集し、学習用データとして利用することは、法廷写真撮影事件最判が示した基準に照らすと肖像権侵害に該当しないと考えます。これは、AI モデル開発においては、特定の人物肖像を学習に利用していますが、大量のデータのごく一部としてしか利用しておらず、かつ AI 開発者は、当該特定の人物肖像を学習に利用していることを認識していないことがほとんどだと思われるからです。もっとも、本ガイドラインでは保守的に考えて、著作権・パブリシティ権と同様、「学習用データの同一・類似物が AI 生成物として生成される事態が頻発するような手法の学習（例：過学

習）を行わない。」旨定めています。

また、ヴァーチャルヒューマン生成 AI サービスの利用者による肖像権侵害が生じることを防止するために、著作権と同様、本ガイドラインにおいては「②サービス利用者が特定の著作権者の著作物、特定の著名人・個人の肖像等を生成することができないよう、特定の著作権者の名称、特定の作品名、キャラクター名、著名人の氏名・芸名、実在の人物の個人氏名等をタグ・ラベルとして用いた学習を行わない」ことも合わせて定めています。

（2） 検証可能性の確保

AI 事業者 GL 上、AI 開発者が AI モデルを開発するに際して遵守すべき事項として以下が定められています。

・ AI の判断にかかわる検証可能性を確保するため、データ量又はデータ内容に照らし合理的な範囲で、AI システム・サービスの開発過程、利用時の入出力等、AI の学習プロセス、推論過程、判断根拠等のログを記録・保存する（AI 事業者 GL P 18）

・ ログの記録・保存にあたっては、利用する技術の特性及び用途に照らして、事故の原因究明、再発防止策の検討、損害賠償責任要件の立証上の重要性等を踏まえて、記録方法、頻度、保存期間等について検討する（同）

・ AI の予測性能及び出力の品質が、活用開始後に大きく変動する可能性又は想定する精度に達しないこともある特性を踏まえ、事後検証のための作業記録を保存しつつ、その品質の維持・向上を行う（「2）安全性」、「6）透明性」）（同 P 29）

本項はこれに対応した条項です。

この「検証可能性の確保」は、「透明性」（AI 事業者 GL P 18）の要請に基づくものですが、AI 開発者にこの見地から重い義務を課すと、AI 開発の支障となりかねません。そのため AI 事業者 GL においても「データ量又はデータ内容に照らし合理的な範囲で」という留保が付されているものと思われます。

そこで、本ガイドラインにおいては、AI 事業者 GL と同様「「データ量又はデータ内容に照らし合理的な範囲で」という留保を付すと同時に、ログの記録・保存が各開発・提供事業者における努力義務であることを明確化しました。

3 AI サービス提供時

（1） 技術的措置

開発・提供事業者は、利用者による知的財産権等の侵害が生じないよう、サービス提供に際して以下の技術的措置をとるものとします。

① 利用者が、特定の著作権者の名称、特定の作品名、キャラクター名、著名人の氏名・芸名、実在の人物の個人氏名等を属性・プロンプトとして入力できないようにする措置

② 学習用データと AI 生成物の類似度をチェックし、一定の閾値以上の類似度の AI 生成物が出力されないようにする措置

（2） サービス利用規約によるコントロール

開発・提供事業者は、利用者による知的財産権等の侵害が生じないよう、サービス提供に関するサービス利用規約内に以下の禁止事項を定めるものとします。

① 特定の著作権者の名称、特定の作品名、キャラクター名、著名人の氏名・芸名、実在の人物の個人氏名等をプロンプトとして入力する行為の禁止

② 既存の著作物、著名人の肖像、実在個人の肖像等と類似する AI 生成物生成の禁止

③ 既存の著作物、著名人の肖像、実在個人の肖像等と類似する AI 生成物が仮に生成された場合において、それらの AI 生成物を利用（複製や販売、ウェブサイトへのアップロード等）することの禁止

④ AI 生成物をアダルト目的で利用・販売等することの禁止

(3) 利用者への情報提供

開発・提供事業者は、利用者に対し、以下の情報を適時かつ適切に提供するよう努めなければなりません。

① AI を利用しているという事実及び適切/不適切な使用方法等

② AI システム・サービスの学習等による出力又はプログラムの変化の可能性があること

③ AI システム・サービスの動作状況に関する情報、不具合が生じた場合の原因及び対応状況等

④ AI モデルにて学習するデータの収集ポリシー、学習方法、実施体制等

【解説】

フルスクラッチ型サービスにおいては、開発・提供事業者は AI 開発者であると同時に AI 提供者にも該当します。そのため、開発・提供事業者は AI サービス提供時にも AI 提供者としての各種義務を遵守する必要があります。

具体的には（1）技術的措置（2）サービス利用規約によるコントロール（3）利用者への情報提供の 3 点です。（1）及び（2）は、サービス利用者による第三者の知的財産権等の侵害発生可能性を低減する措置、（3）は AI 事業者 GL 上の「透明性」に由来する要請事項です。

(1) 技術的措置

ヴァーチャルヒューマン生成 AI サービスの利用者は、何らかの属性（年齢や性別）、プロンプトをサービスに入力して AI 生成物を生成して受領します。

そのため、利用者による第三者の知的財産権等の侵害発生可能性を低減する技術的措置としては、①利用者による属性・プロンプト入力時のコントロールと、②AI 生成物の利用者による受領時点でのコントロールが存在します。

そこで、本ガイドラインにおいては「利用者による属性・プロンプト入力時のコントロール」として、「① 利用者が、特定の著作権者の名称、特定の作品名、キャラクター名、著名人の氏名・芸名、実在の人物の個人氏名等を属性・プロンプトとして入力できないように

する措置」を、「AI 生成物の利用者による受領時点でのコントロール」として「学習用データと AI 生成物の類似度をチェックし、一定の閾値以上の類似度の AI 生成物が出力されないようにする措置」を義務づけました。

もちろん、いずれの技術的措置も、実際にどのような技術要素を用いて実現するかは各開発・提供事業者に委ねられていますし、コントロールについて一定以上の精度を義務づけるものでもありません。

（2） サービス利用規約によるコントロール

また、開発・提供事業者がヴァーチャルヒューマン生成 AI サービスを利用者に対して提供する際には、当該サービスの利用規約を利用者との間で締結するのが通常です。利用者による第三者の知的財産権等の侵害発生可能性を低減するためには、当該サービス利用規約において利用者に具体的な禁止事項を義務づけることも有効です。

そこで、本ガイドラインにおいては、サービス利用規約において定めるべき禁止事項について列挙しました。

（3） 利用者への情報提供

AI 事業者 GL 上、AI 提供者が A サービスを提供するに際して遵守すべき事項として以下が定められています。

P-6）ii. 関連するステークホルダーへの情報提供（AI 事業者 GL P 34）

▼ 提供する AI システム・サービスについて、例えば以下の事項を平易かつアクセスしやすい形で、適時かつ適切に情報を提供する（「6）透明性」）

・ AI を利用しているという事実、活用している範囲、適切/不適切な使用方法等（「6）透明性」）

・ 提供する AI システム・サービスの技術的特性、利用によりもたらす結果より生じる可能性のある予見可能なリスク及びその緩和策等の安全性に関する情報（「2）安全性」）

・ AI システム・サービスの学習等による出力又はプログラムの変化の可能性（「1）人間中心」）

・ AI システム・サービスの動作状況に関する情報、不具合の原因及び対応状況、インシデント事例等（「2）安全性」）

・ AI システムの更新を行った場合の更新内容及びその理由の情報（「2）安全性」）

・ AI モデルにて学習するデータの収集ポリシー、学習方法、実施体制等（「3）公平性」、「4）プライバシー保護」、「5）セキュリティ確保」）

もっともこの「関連するステークホルダーへの情報提供」は、開発・提供事業者におけるプライバシー及び営業秘密へ配慮しつつ、採用する技術の特性及び用途に照らし合理的な範囲で実施することが期待されているものです（AI 事業者 GL 別添（付属資料）P 91，104 参照）。

そこで、本ガイドラインにおいては、上記 AI 事業者 GL を参照しつつ、ヴァーチャルヒューマン生成 AI サービスの開発・提供事業者として現実的に対応可能な措置に絞って努力義務として列挙しました。

第５　外部モデル利用型サービス

1　技術的措置

開発・提供事業者は、利用者による知的財産権等の侵害が生じないよう、サービス提供に際して以下の技術的措置をとるものとします。

①　利用者が、特定の著作権者の名称、特定の作品名、キャラクター名、著名人の氏名・芸名、実在の人物の個人氏名等を属性・プロンプトとして入力できないようにする措置

②　学習用データと AI 生成物の類似度をチェックし、一定の閾値以上の類似度の AI 生成物が出力されないようにする措置

2　サービス利用規約によるコントロール

開発・提供事業者は、利用者による知的財産権等の侵害が生じないよう、サービス提供に関するサービス利用規約内に以下の禁止事項を定めるものとします。

①　特定の著作権者の名称、特定の作品名、キャラクター名、著名人の氏名・芸名、実在の人物の個人氏名等をプロンプトとして入力する行為の禁止

②　既存の著作物、著名人の肖像、実在個人の肖像等と類似する AI 生成物生成の禁止

③　既存の著作物、著名人の肖像、実在個人の肖像等と類似する AI 生成物が仮に生成された場合において、それらの AI 生成物を利用（複製や販売、ウェブサイトへのアップロード等）することの禁止

④　AI 生成物をアダルト目的で利用・販売等することの禁止

3　利用者への情報提供

開発・提供事業者は、利用者に対し、以下の情報を適時かつ適切に提供するよう努めなければなりません。

①　AI を利用しているという事実及び適切/不適切な使用方法等

②　AI システム・サービスの学習等による出力又はプログラムの変化の可能性があること

③　AI システム・サービスの動作状況に関する情報、不具合が生じた場合の原因及び対応状況等

4　システムアーキテクチャ等の文書化

開発・提供事業者は、AI の入出力等の説明可能性を確保するため、AI システムの入出力等のログを記録・保存し、解釈可能な内容で文書化するよう努めなければなりません。

【解説】

外部モデル利用型サービスにおいては、開発・提供事業者は AI 提供者にのみ該当し、AI 開発者には該当しません。したがって、外部モデル利用型サービスの開発・提供事業者が遵

守すべき遵守事項は、フルスクラッチ型サービスの開発・提供事業者における「第 4・3　AI サービス提供時」の遵守事項と基本的には同一となります。

具体的には（1）技術的措置（2）サービス利用規約によるコントロール（3）利用者への情報提供の 3 点です。

一方、本ガイドラインでは、外部モデル利用型サービス特有の遵守事項として「4　システムアーキテクチャ等の文書化」を遵守する努力義務を課しています。

1　技術的措置

ヴァーチャルヒューマン生成 AI サービスの利用者は、何らかのプロンプトをサービスに入力して AI 生成物を生成して受領します。

そのため、利用者による第三者の知的財産権等の侵害発生可能性を低減する技術的措置としては、①利用者による属性・プロンプト入力時のコントロールと、②AI 生成物の利用者による受領時点でのコントロールが存在します。

そこで、本ガイドラインにおいては「利用者による属性・プロンプト入力時のコントロール」として、「①　利用者が、特定の著作権者の名称、特定の作品名、キャラクター名、著名人の氏名・芸名、実在の人物の個人氏名等をプロンプトとして入力できないようにする措置」、「AI 生成物の利用者による受領時点でのコントロール」として「学習用データと AI 生成物の類似度をチェックし、一定の閾値以上の類似度の AI 生成物が出力されないようにする措置」を義務づけました。

もちろん、いずれの技術的措置も、実際にどのような技術要素を用いて実現するかは各開発・提供事業者に委ねられていますし、コントロールについて一定以上の精度を義務づけるものでもありません。

2　サービス利用規約によるコントロール

また、開発・提供事業者がヴァーチャルヒューマン生成 AI サービスを利用者に対して提供する際には、当該サービスの利用規約を利用者との間で締結するのが通常です。利用者による第三者の知的財産権等の侵害発生可能性を低減するためには、当該サービス利用規約において利用者に具体的な禁止事項を義務づけることも有効です。

そこで、本ガイドラインにおいては、サービス利用規約において定めるべき禁止事項について列挙しました。3　利用者への情報提供

AI 事業者 GL 上、AI 提供者が A サービスを提供するに際して遵守すべき事項として以下が定められています。

P-6）ii. 関連するステークホルダーへの情報提供（AI 事業者 GL P 34）

▼　提供する AI システム・サービスについて、例えば以下の事項を平易かつアクセスしやすい形で、適時かつ適切に情報を提供する（「6）透明性」）

・　AI を利用しているという事実、活用している範囲、適切/不適切な使用方法等（「6）透明性」）

・　提供する AI システム・サービスの技術的特性、利用によりもたらす結果より生じる可能性のある予見可能なリスク及びその緩和策等の安全性に関する情報（「2）安全性」）

・　AI システム・サービスの学習等による出力又はプログラムの変化の可能性（「1）人間中心」）
・　AI システム・サービスの動作状況に関する情報、不具合の原因及び対応状況、インシデント事例等（「2）安全性」）
・　AI システムの更新を行った場合の更新内容及びその理由の情報（「2）安全性」）
・　AI モデルにて学習するデータの収集ポリシー、学習方法、実施体制等（「3）公平性」、「4）プライバシー保護」、「5）セキュリティ確保」）

もっともこの「関連するステークホルダーへの情報提供」は、開発・提供事業者におけるプライバシー及び営業秘密へ配慮しつつ、採用する技術の特性及び用途に照らし合理的な範囲で実施することが期待されているものです（AI 事業者 GL 別添（付属資料）P 91，104 参照）。

そこで、本ガイドラインにおいては、上記 AI 事業者 GL を参照しつつ、ヴァーチャルヒューマン生成 AI サービスの開発・提供事業者として現実的に対応可能な措置に絞って努力義務として列挙しました。

4　システムアーキテクチャ等の文書化

AI 事業者 GL 上、AI 提供者が A サービスを提供するに際して遵守すべき事項として以下が定められています。

P-6）ｉ．システムアーキテクチャ等の文書化（AI 事業者 GL P 34）
トレーサビリティ及び透明性の向上のため、意思決定に影響を与える提供する AI システム・サービスのシステムアーキテクチャ、データの処理プロセス等について文書化する（「6）透明性」）

さらに、AI 事業者 GL 上は、同事項に関する「ポイント」として以下の内容が記載されています。

［ポイント］（AI 事業者 GL 別添（付属資料）P 123）
AI 提供者は、AI の入出力等の説明可能性を確保するため、AI システムの入出力等のログを記録・保存し、解釈可能な内容で文書化すると、プロセス自体の改善も容易になり、関連するステークホルダーとのコミュニケーション及び対話が強化される。必要に応じて、リスク管理文書を公開する。文書化により透明性が高まり、人によるレビュープロセスが可能になることで説明可能性の確保につながる。

そこで、本ガイドラインにおいては、上記 AI 事業者 GL を参照しつつ、ヴァーチャルヒューマン生成 AI サービスの開発・提供事業者として現実的に対応可能な措置に絞って努力義務として記載しました。

第 6　追加学習型サービス

1　前提条件
本ガイドラインのうち AI の開発に関連する事項については AI 開発者のデータ収集・学

習行為に日本国の法令が適用されることを前提としています。そのため、開発・提供事業者が学習用データの収集及びAIモデルの学習を行うに際しては、日本国内にあるサーバを用いて、日本国内に所在する作業者により作業を行ってください。

【解説】

本ガイドラインのうち、AIの開発に関連する事項については、AI開発者の各種行為（データ収集及び学習行為）に日本国の法令が適用されることを前提としています。日本国の各種法令が適用される条件は様々ですが、AI開発において最も重要と思われる著作権法については、利用対象著作物の「利用行為地」の法令が適用されます。そのため、本ガイドラインにおいては、学習用データの収集及び学習に際しては、日本国内にあるサーバを用いて、日本国内に所在する作業者により作業を行うことを義務づけています。

2　追加学習用データ収集・前処理時

開発・提供事業者は以下のデータを追加学習用データとして収集・利用してはなりません。

記

児童ポルノ（児童買春、児童ポルノに係る行為等の規制及び処罰並びに児童の保護等に関する法律第2条に定める「児童ポルノ」をいう）

以上

【解説】

AI事業者GL上、AI開発者が学習用データの収集・利用に際して遵守すべき事項として以下が定められています。

・　学習等に用いるデータの透明性の確保、法的枠組みの遵守、AIモデルの更新等を合理的な範囲で適切に実施する（AI事業者GL P16）

・　プライバシー・バイ・デザイン等を通じて、学習時のデータについて、適正に収集するとともに、第三者の個人情報、知的財産権に留意が必要なもの等が含まれている場合には、法令に従って適切に扱うことを、AIのライフサイクル全体を通じて確保する（同P28）

本項はこれに対応した条項です。

(1)　原則

日本の法令が適用される限りにおいて、特定のデータを学習用データとして収集・利用すること自体が何らかの法令違反や知的財産権の侵害になることは原則としてはありません。

(2)　例外

もっとも、児童ポルノ（児童買春、児童ポルノに係る行為等の規制及び処罰並びに児童の保護等に関する法律第2条に定める「児童ポルノ」をいう）については、自己の性的好奇心を満たす目的で所持すること自体が刑事罰の対象となっています（同法7条1項）。

そのため、本ガイドラインにおいては児童ポルノについては学習用データとして収集・利

用することを禁止しています。

3　追加学習時

（1）　適正追加学習

開発・提供事業者による AI モデルの追加学習自体が第三者の知的財産権等の侵害に該当すること、及び開発・提供事業者が開発したサービスを AI 利用者が利用することで第三者の知的財産権等の侵害が生じることのないよう、開発・提供事業者は AI モデルの追加学習時には以下の点を遵守しなければなりません。

①　追加学習用データの同一・類似物が AI 生成物として生成される事態が頻発するような手法の追加学習（例：過学習）を行わない。

②　サービス利用者が特定の著作権者の著作物、特定の著名人・個人の肖像等を生成することができないよう、特定の著作権者の名称、特定の作品名、キャラクター名、著名人の氏名・芸名、実在の人物の個人氏名等をタグ・ラベルとして用いた追加学習を行わない

（2）　検証可能性の確保

開発・提供事業者は、AI の判断にかかわる検証可能性を確保するため、データ量又はデータ内容に照らし合理的な範囲で、AI システム・サービスの開発過程、利用時の入出力等、AI の追加学習プロセス、推論過程、判断根拠等のログを記録・保存するよう努めなければなりません。

【解説】

（1）　適正追加学習

AI 事業者 GL 上、AI 開発者が AI モデルを開発するに際して遵守すべき事項として以下が定められています。

・　学習等に用いるデータの透明性の確保、法的枠組みの遵守、AI モデルの更新等を合理的な範囲で適切に実施する（AI 事業者 GL P16）

・　プライバシー・バイ・デザイン等を通じて、学習時のデータについて、適正に収集するとともに、第三者の個人情報、知的財産権に留意が必要なもの等が含まれている場合には、法令に従って適切に扱うことを、AI のライフサイクル全体を通じて確保する（同 P28）

本項はこれに対応した条項です。

ア　ヴァーチャルヒューマン生成 AI サービスの開発・提供に際して問題となる法的権利等

ヴァーチャルヒューマン生成 AI サービスの開発・提供に際して問題となることが多い法的権利・法規制等は、①　著作権、②　パブリシティ権、③　肖像権、④　児童ポルノです。このうち「④　児童ポルノ」については、本ガイドラインにおいてはそもそも追加学習用データとして収集・利用することを禁止しているので、AI モデル開発時には特段問題となりません。

また、ヴァーチャルヒューマン生成 AI サービスの開発・提供に際しては、実在の人間の顔写真を収集・利用することもありますが、実在の人間の顔写真は「個人情報」（個人情報保護法第 2 条 1 項）に該当します。もっとも、企業が個人情報を取得して利用する場合には、予め利用目的を特定したうえで公表等し、当該目的の範囲内で利用すれば問題ありません。そのため本ガイドラインでは個人情報の点については特段言及していません。

イ　2 つの視点

ヴァーチャルヒューマン生成 AI サービスの開発・提供に際して、第三者の知的財産権の侵害が生じないようにすることを考える場合、2 つの視点があります。

一つは、開発・提供事業者による AI モデルの追加学習自体が第三者の知的財産権等の侵害に該当する（直接侵害）ことがないようにする（直接侵害の防止）という視点、もう 1 つは、開発・提供事業者が開発したサービスを AI 利用者が利用することが第三者の知的財産権等の侵害に該当する（間接侵害）ことがないようにする（間接侵害の防止）という視点です。

このうち、前者の直接侵害が生じないようにすることは開発・提供事業者にとって当然の義務です。

一方、後者の間接侵害については、仮に AI 利用者が AI モデル・サービスを利用することで第三者の知的財産権等の侵害が生じたとしても、必ずしも当該 AI モデル・サービスを開発・提供した開発・提供事業者自身が法的責任を問われるとは限りません。また、間接侵害が生じるか否かは AI 利用者の AI モデル・サービスの利用方法に依拠するところが多いため、AI 開発者が間接侵害を完全に防止することは不可能です。その意味で、後者の間接侵害が生じないようにすることは開発・提供事業者にとって法的な義務とまでは評価できません。もっとも、ヴァーチャルヒューマン生成 AI サービスが社会に広く受容されていくためには、間接侵害も生じないよう、開発・提供事業者ができるだけのことをすることが求められているといえるでしょう。

ウ　著作権

人間が創作した著作物（イラスト、写真等）に関して発生する権利です。ヴァーチャルヒューマン生成 AI サービスの開発・提供に際しては、第三者が創作したイラストや写真を収集・利用することも多いため著作権侵害に該当しないような対応が必要です。

日本の著作権法が適用される限りにおいて、第三者の著作物を AI モデル開発のような「情報解析」に利用することは原則として適法です（著作権法第 30 条の 4 第 2 号）。もっとも、追加学習対象著作物の利用に際して、「学習」という「情報解析」の目的に加えて、当該著作物の同一・類似物を出力させることを目的（表現出力目的）としている場合には、30 条の 4 は適用されません。

「考え方」においては、この表現出力目的の具体例として「AI 開発事業者又は AI サービス提供事業者が、AI 追加学習に際して、いわゆる「過学習」（overfitting）を意図的に行う場合」を挙げ（「考え方」20 頁）、さらに、AI 生成物の生成・利用段階で「学習された著作物と創作的表現が共通した生成物の生成が著しく頻発するといった事情」があれば、「表

現出力目的」が推認されるとしています（「考え方」２１頁）。

そこで、本ガイドラインにおいては、「①　追加学習用データの同一・類似物がAI生成物として生成される事態が頻発するような手法の追加学習（例：過学習）を行わない。」ことを定めています。

さらに、ヴァーチャルヒューマン生成AIサービスの利用者による著作権侵害(間接侵害)が生じることを防止するために、本ガイドラインにおいては「②サービス利用者が特定の著作権者の著作物、特定の著名人・個人の肖像等を生成することができないよう、特定の著作権者の名称、特定の作品名、キャラクター名、著名人の氏名・芸名、実在の人物の個人氏名等をタグ・ラベルとして用いた追加学習を行わない」ことも合わせて定めています。

エ　パブリシティ権

（ア）　パブリシティ権とは

パブリシティ権とは、人の氏名、肖像等が有する顧客吸引力を排他的に利用する権利として最判平成24年2月2日（民集66巻2号89頁、いわゆるピンク・レディー事件）により認められた法的権利です。

具体的には、ピンク・レディー事件最高裁判決（以下「ピンク最判」といいます）は、①氏名，肖像等それ自体を独立して鑑賞の対象となる商品等として使用し，②商品等の差別化を図る目的で氏名，肖像等を商品等に付し，③氏名，肖像等を商品等の広告として使用するなど，「専ら氏名，肖像等の有する顧客吸引力の利用を目的とするといえる場合」には、パブリシティ権侵害として不法行為上違法になると判示しました（以下、ピンク最判が示した3種類の侵害類型を「侵害三類型」といいます)。

あくまで、「人の氏名、肖像等が有する顧客吸引力を排他的に利用する権利」ですので、パブリシティ権を有するのはいわゆる著名人・有名人に限られます。著名人・有名人でなければ、その氏名、肖像等に顧客吸引力が生じることはないからです。この点は「エ　肖像権」で説明する肖像権との大きな違いです。

（イ）　AI開発等とパブリシティ権侵害

まず、AI開発のために著名人の肖像等を収集し、追加学習用データとして利用することはピンク最判が示した「侵害三類型」に該当しません。もっとも、本ガイドラインでは保守的に考えて、著作権と同様、「追加学習用データの同一・類似物がAI生成物として生成される事態が頻発するような手法の追加学習（例：過学習）を行わない。」旨定めています。

また、ヴァーチャルヒューマン生成AIサービスの利用者によるパブリシティ権侵害が生じることを防止するために、著作権と同様、本ガイドラインにおいては「②サービス利用者が特定の著作権者の著作物、特定の著名人・個人の肖像等を生成することができないよう、特定の著作権者の名称、特定の作品名、キャラクター名、著名人の氏名・芸名、実在の人物の個人氏名等をタグ・ラベルとして用いた追加学習を行わない」ことも合わせて定めています。

オ　肖像権

（ア）　肖像権とは

肖像権とは、最も広く捉えると「人の容ぼう、姿態（以下併せて「容ぼう等」という）に関する権利ないし人格的利益」を指します。

我が国ではこれを認める明文規定がありませんが、最判昭和 44 年 12 月 24 日（刑集 23 巻 12 号 1625 頁、いわゆる京都府学連デモ事件）及び最判平成 17 年 11 月 10 日（民集 59 巻 9 号 2428 頁、いわゆる法廷写真撮影事件）において、肖像権ないし肖像に関する人格的利益が法的保護に値するものであることは明確に認められています。

なお、肖像権についてはパブリシティ権と異なり一般人についても認められます。

もっとも、一般人の容ぼう等を何らかの方法で利用した場合（たとえば無断撮影や、撮影した写真を雑誌やインターネットに掲載すること）に直ちに肖像権侵害に該当する訳ではありません。

法廷写真撮影事件において、最高裁は「人は，みだりに自己の容ぼう等を撮影されないということについて法律上保護されるべき人格的利益を有する（最高裁昭和 40 年(あ)第 1187 号同 44 年 12 月 24 日大法廷判決・刑集 23 巻 12 号 1625 頁参照)。」として、人の容ぼう等の撮影行為及び同撮影された写真の公表行為の違法性の判断基準として以下のとおり判示しました。

(1) 撮影行為の違法性判断基準

同判決は、人の容ぼう等の撮影行為の違法性判断基準として「ある者の容ぼう等をその承諾なく撮影することが不法行為法上違法となるかどうかは，被撮影者の社会的地位，撮影された被撮影者の活動内容，撮影の場所，撮影の目的，撮影の態様，撮影の必要性等を総合考慮して，被撮影者の上記人格的利益の侵害が社会生活上受忍の限度を超えるものといえるかどうかを判断して決すべきである。」としました。

(2) 撮影した写真の公表行為の違法性判断基準

また、同時に本判決は「また，人は，自己の容ぼう等を撮影された写真をみだりに公表されない人格的利益も有すると解するのが相当であり，人の容ぼう等の撮影が違法と評価される場合には，その容ぼう等が撮影された写真を公表する行為は，被撮影者の上記人格的利益を侵害するものとして，違法性を有するものというべきである。」として、人が「自己の容ぼう等を撮影された写真をみだりに公表されない人格的利益」を有すること、及び人の容ぼう等の撮影行為が違法である場合には、当該写真の公表も違法であることについても判示しました。

（イ）　AI 開発等と肖像権侵害

まず、AI モデルの開発のために一般人の肖像等を収集し、追加学習用データとして利用することは、法廷写真撮影事件最判が示した基準に照らすと肖像権侵害に該当しないと考えます。これは、AI モデル開発においては、特定の人物肖像を追加学習に利用しています

が、大量のデータのごく一部としてしか利用しておらず、かつ AI 開発者は、当該特定の人物肖像を追加学習に利用していることを認識していないことがほとんどだと思われるからです。もっとも、本ガイドラインでは保守的に考えて、著作権・パブリシティ権と同様、「追加学習用データの同一・類似物が AI 生成物として生成される事態が頻発するような手法の追加学習（例：過学習）を行わない。」旨定めています。

また、ヴァーチャルヒューマン生成 AI サービスの利用者による肖像権侵害が生じることを防止するために、著作権と同様、本ガイドラインにおいては「②サービス利用者が特定の著作権者の著作物、特定の著名人・個人の肖像等を生成することができないよう、特定の著作権者の名称、特定の作品名、キャラクター名、著名人の氏名・芸名、実在の人物の個人氏名等をタグ・ラベルとして用いた追加学習を行わない」ことも合わせて定めています。

(2)　検証可能性の確保

AI 事業者 GL 上、AI 開発者が AI モデルを開発するに際して遵守すべき事項として以下が定められています。

・　AI の判断にかかわる検証可能性を確保するため、データ量又はデータ内容に照らし合理的な範囲で、AI システム・サービスの開発過程、利用時の入出力等、AI の学習プロセス、推論過程、判断根拠等のログを記録・保存する（AI 事業者 GL P 18）

・ ログの記録・保存にあたっては、利用する技術の特性及び用途に照らして、事故の原因究明、再発防止策の検討、損害賠償責任要件の立証上の重要性等を踏まえて、記録方法、頻度、保存期間等について検討する（同）

・　AI の予測性能及び出力の品質が、活用開始後に大きく変動する可能性又は想定する精度に達しないこともある特性を踏まえ、事後検証のための作業記録を保存しつつ、その品質の維持・向上を行う（「2）安全性」、「6）透明性」）（同 P 29）

本項はこれに対応した条項です。

この「検証可能性の確保」は、「透明性」（AI 事業者 GL P 18）の要請に基づくものですが、AI 開発者にこの見地から重い義務を課すと、AI 開発の支障となりかねません。その見地から、AI 事業者 GL においても「データ量又はデータ内容に照らし合理的な範囲で」という留保が付されているものと思われます。

そこで、本ガイドラインにおいては、AI 事業者 GL と同様「「データ量又はデータ内容に照らし合理的な範囲で」という留保を付すと同時に、ログの記録・保存が各開発・提供事業者における努力義務であることを明確化しました。

4　AI サービス提供時

(1)　技術的措置

開発・提供事業者は、利用者による知的財産権等の侵害が生じないよう、サービス提供に際して以下の技術的措置をとるものとします。

①　利用者が、特定の著作権者の名称、特定の作品名、キャラクター名、著名人の氏名・芸名、実在の人物の個人氏名等を属性・プロンプトとして入力できないようにする措置

② 追加学習用データと AI 生成物の類似度をチェックし、一定の閾値以上の類似度の AI 生成物が出力されないようにする措置

(2) サービス利用規約によるコントロール

開発・提供事業者は、利用者による知的財産権等の侵害が生じないよう、サービス提供に関するサービス利用規約内に以下の禁止事項を定めるものとします。

① 特定の著作権者の名称、特定の作品名、キャラクター名、著名人の氏名・芸名、実在の人物の個人氏名等をプロンプトとして入力する行為の禁止

② 既存の著作物、著名人の肖像、実在個人の肖像等と類似する AI 生成物生成の禁止

③ 既存の著作物、著名人の肖像、実在個人の肖像等と類似する AI 生成物が仮に生成された場合において、それらの AI 生成物を利用（複製や販売、ウェブサイトへのアップロード等）することの禁止④ AI 生成物をアダルト目的で利用・販売等することの禁止

(3) 利用者への情報提供

開発・提供事業者は、利用者に対し、以下の情報を適時かつ適切に提供するよう努めなければなりません。

① AI を利用しているという事実及び適切/不適切な使用方法等

② AI システム・サービスの追加学習等による出力又はプログラムの変化の可能性があること

③ AI システム・サービスの動作状況に関する情報、不具合が生じた場合の原因及び対応状況等

④ AI モデルにて追加学習に用いるデータの収集ポリシー、追加学習方法、実施体制等

【解説】

フルスクラッチ型サービスにおいては、開発・提供事業者は AI 開発者であると同時に AI 提供者にも該当します。そのため、開発・提供事業者は AI サービス提供時にも各種義務を遵守する必要があります。

具体的には（1）技術的措置（2）サービス利用規約によるコントロール（3）利用者への情報提供の 3 点です。(1) 及び (2) は、サービスを利用する利用者による第三者の知的財産権等の侵害発生可能性を低減する措置、(3) は AI 事業者 GL 上の「透明性」に由来する要請事項です。

(1) 技術的措置

ヴァーチャルヒューマン生成 AI サービスの利用者は、何らかの属性・プロンプトをサービスに入力して AI 生成物を生成して受領します。

そのため、利用者による第三者の知的財産権等の侵害発生可能性を低減する技術的措置としては、①利用者によるプロンプト入力時のコントロールと、②AI 生成物の利用者による受領時点でのコントロールが存在します。

そこで、本ガイドラインにおいては「利用者による属性・プロンプト入力時のコントロール」として、「① 利用者が、特定の著作権者の名称、特定の作品名、キャラクター名、著名人の氏名・芸名、実在の人物の個人氏名等を属性・プロンプトとして入力できないようにする措置」、「AI 生成物の利用者による受領時点でのコントロール」として「追加学習用データと AI 生成物の類似度をチェックし、一定の閾値以上の類似度の AI 生成物が出力されないようにする措置」を義務づけました。

もちろん、いずれの技術的措置も、実際にどのような技術要素を用いて実現するかは各開発・提供事業者に委ねられていますし、コントロールについて一定以上の精度を義務づけるものでもありません。

(2) サービス利用規約によるコントロール

また、開発・提供事業者がヴァーチャルヒューマン生成 AI サービスを利用者に対して提供する際には、当該サービスの利用規約を利用者との間で締結するのが通常です。利用者による第三者の知的財産権等の侵害発生可能性を低減するためには、当該サービス利用規約において利用者に具体的な禁止事項を義務づけることも有効です。

そこで、本ガイドラインにおいては、サービス利用規約において定めるべき禁止事項について列挙しました。

(3) 利用者への情報提供

AI 事業者 GL 上、AI 提供者が A サービスを提供するに際して遵守すべき事項として以下が定められています。

P-6）ii. 関連するステークホルダーへの情報提供（AI 事業者 GL P 34）

▼ 提供する AI システム・サービスについて、例えば以下の事項を平易かつアクセスしやすい形で、適時かつ適切に情報を提供する（「6）透明性」）

・ AI を利用しているという事実、活用している範囲、適切/不適切な使用方法等（「6）透明性」）

・ 提供する AI システム・サービスの技術的特性、利用によりもたらす結果より生じる可能性のある予見可能なリスク及びその緩和策等の安全性に関する情報（「2）安全性」）

・ AI システム・サービスの学習等による出力又はプログラムの変化の可能性（「1）人間中心」）

・ AI システム・サービスの動作状況に関する情報、不具合の原因及び対応状況、インシデント事例等（「2）安全性」）

・ AI システムの更新を行った場合の更新内容及びその理由の情報（「2）安全性」）

・ AI モデルにて学習するデータの収集ポリシー、学習方法、実施体制等（「3）公平性」、「4）プライバシー保護」、「5）セキュリティ確保」）

もっともこの「関連するステークホルダーへの情報提供」は、開発・提供事業者におけるプライバシー及び営業秘密へ配慮しつつ、採用する技術の特性及び用途に照らし合理的な範囲で実施することが期待されているものです（AI 事業者 GL 別添（付属資料）P 91，104 参照）。

そこで、本ガイドラインにおいては、上記 AI 事業者 GL を参照しつつ、ヴァーチャルヒューマン生成 AI サービスの開発・提供事業者として現実的に対応可能な措置に絞って努力義務として列挙しました。

以上