

https://www.meti.go.jp/shingikai/mono_info_service/ai_utilization/

『OpenAI（ChatGPT）の企業向け約款等で個人情報保護・セキュリティ上気になる点の
まとめ』

2024/12/23 検討会 委員 IPA 登 大遊

メールアドレス: d-nobori.m1@mail1.cyber.ipa.go.jp

2025/01/15 一部加筆修正

■ この意見書を作成した理由

1. 日本企業が活用したいと考えている AI サービスのうち、人気があるものの 1 つに、米国 OpenAI 社の ChatGPT あるいはその API サービスがあります。
2. この機会に、OpenAI の以下のプライバシーポリシーや企業向け約款の全文を、企業の担当者の視点を想定して、詳しく読んでみました。

- ・ 『OpenAI Business terms（OpenAI 企業向け約款） November 14, 2023』
原文: <https://openai.com/policies/business-terms/>
- ・ 『OpenAI Privacy policy November 4, 2024 版』
原文: <https://openai.com/policies/privacy-policy/>
- ・ 『Data Processing Addendum（データ処理委託特約） February 15, 2024 版』
原文: <https://openai.com/policies/data-processing-addendum/>
- ・ 『OpenAI における企業プライバシー 2024 年 10 月 31 日版』
原文: <https://openai.com/ja-JP/enterprise-privacy/>

すると、個人情報保護・セキュリティ上、気になる点がいくつかありました。それらを、下記にまとめました。われわれ日本人・日本企業が、どのようにすればこの問題を根本的に解決でき、個人情報保護やセキュリティに配慮しつつ、AI 技術による大きな利益を手に入れることができるのかについても、末尾に少しまとめました。

なお、OpenAI の AI サービスを、企業向けの API インターフェイスを呼び出す場合には、上記のうち、『OpenAI Privacy policy』は適用されないと記載があります。ただし、企業ユーザーであっても、API を用いずに、OpenAI の ChatGPT の通常の画面・通常の契約で個人データを分析するケースも相当程度存在すると思われることから、『OpenAI Privacy policy』についても、分析の対象としました。

(1) 企業向け約款は、顧客が OpenAI のサービスを個人データを取り扱うために利用することが想定されて記載されている（→ OpenAI 企業向け約款 6.1 節）。学習をオプトアウトしても、単にモデル学習に利用されなくなるだけで、その他の目的では利用されるし（OpenAI における企業プライバシー「サービス全般」の「Q. OpenAI は顧客のビジネスデータの検証を行いますか?」）、また、米国カリフォルニア州法あるいは米国法が要求する場合は、第三者に開示されてしまうことになっている（→ データ処理委託特約 2 節, 8 節、OpenAI Privacy policy 2 節）。個人情報保護委員会の、いわゆる「クラウド例外」においては、「…クラウドサービス提供事業者が、当該個人データを取り扱わないこととなっている場合」には、本人の同意が必要な第三者提供や委託に該当しないものとされている。一部の日本ユーザー企業側は、AI サービスに個人情報を分析させる際、この「クラウド例外」を用いて、日本の個人情報保護法（以下「法」）が義務付ける、個人データの取扱いを第三者に委託する際に必要な各種の安全監理を免れることができるという期待を持っているようである。

https://www.ppc.go.jp/all_faq_index/faq1-q7-53/

しかしながら、OpenAI の企業向け約款に基づけば、この「クラウド例外」が利用できないことになりそうである（※ 1）。すると、原則として法 28 条 1 項の「あらかじめ外国にある第三者への提供を認める旨の本人の同意を得なければならない」が適用されるのではないかと。ただし、法 28 条 1 項の例外として、①「個人の権利利益を保護する上で我が国と同等の水準にあると認められる個人情報の保護に関する制度を有している外国として個人情報保護委員会規則で定めるもの」と②「個人データの取扱いについてこの節の規定により個人情報取扱事業者が講ずべきこととされている措置に相当する措置…を継続的に講ずるために必要なものとして個人情報保護委員会規則で定める基準に適合する体制を整備している者」がある。日本の各ユーザー企業においては、原則、個人データを OpenAI のサービスに当該個人の事前同意なくインプットしようとする場合は、是非ともこれら 2 つの例外を用いたいが、①は EU 及び英国を指すから、米国企業である OpenAI 社には使えない。

そこで、②を充足する必要があることになる。この場合は、各ユーザー企業は、個別に、OpenAI 社が、「個人情報保護委員会規則で定める基準に適合する体制を整備している者」（規則 16 条）にあたるかを厳格に審査しなければならないのではないかと。だが、それは委託先である OpenAI 社に対してそのソフトウェア、システム、セキュリティ、業務状況等を適切に監理する必要性が生じるので、実際、極めて大変ではないか（その大変さについては、後述する）。そうすると、やはり、原則、個人データを OpenAI のサービスにインプットする場合は、各個人の事前同意が必須であるということになるのではないかと。

なお、仮に、OpenAI 社が②を充足しており、法 28 条 1 項の例外にあたる場合であっても、OpenAI 約款によると、ユーザー企業のための目的以外の目的でも、個人データが収集され、第三者開示される可能性があることが規定されているから（詳しくは、下記で述べる）、それを知って個人データをインプットするならば、これは、単なる「委託」（法 27 条 5 項 1 号）に留まらず、「第三者」への「提供」（法 27 条 1 項）に該当してしまい、やはり、個人本人の事前の同意等が必要となるのではないかと。

(2) 損害賠償金額について、重過失・故意をのぞき、顧客が直近で支払った代金 12 ヶ月分しか賠償されない上限規定がある（→ OpenAI 企業向け約款 11 節）。だが、多数の個人データや、営業秘密データ、ファインチューニング用のデータ等を保存していて（あるいは、保存しているつもりでなくても、約款等で定められている目的で勝手に保存されていて）、それらが万一 OpenAI 社から漏えいしてしまうと、ユーザー企業は、被害者である個人等に対して責任を果たさなければならず、場合によっては、莫大な金額の賠償をしなければならない場合もある。

企業が AI を用いて第三者に分析・処理させる入力個人データとして、従来コンピュータで外部処理を委託してきた個人データ内容は、住所、年齢層、契約内容、請求金額等の情報等に留まることが多かった。そのため、第三者に委託目的でインプットされるデータは限定的であった。しかし、OpenAI のような AI サービスの登場により、日本企業は、各個人にかかる過去の購入履歴や行動履歴、趣味・嗜好、ウェブサイト商品閲覧、投稿履歴、コールセンター社員との会話録音内容や個人の側の反応、サポートセンターとの電子メール授受内容に含まれる個人的秘密、通院・治療歴等の病歴といった、個人の内面に深く関わる機微な多数の情報を AI にインプットし、分析結果のアウトプットを得る、という AI 利用をさかんに行なうようになる。できるだけ多くのデータを第三者にインプットしたほうが、その第三者から、対象となる消費者個人に対する非常に有益なマーケティング分析データを抽出でき、次にその個人を狙った営業戦略を自動的に立案でき、極めて高い営業効果を得られるためである。そこで、企業は、OpenAI 社に対して、これまでの通常のデータ処理委託の際と比べものにならないほどの多量かつ深い個人の内面に関わるデータを、次々に、インプットすることになる。

この場合、OpenAI 社のような極めて能力の高い AI 処理業者から顧客の有する個人データが漏えいした場合の損害は、これまでの一般的ケースと比較して、桁違いに大きくなってしまう。それらのデータの漏えいによる被害者各個人が被る損害はきわめて多額となるためである。

他方で、OpenAI 社の負う責任は、重過失・故意でない限り、わずか直近で支払った代金 12 ヶ月分に限定されてしまい、それを超える責任は負わないとされている。これは、OpenAI 社の技術上や運営上の過失によって対象個人本人に生じた損害の賠償責任について、ユーザー企業各社は、いわば OpenAI 社の代わりに、その大半を負担しなければならないことを意味する。

たしかに、従来から、企業が第三者に対して個人データ処理を委託する場合にも、約款で、損害賠償の上限が、たとえば直近で支払った代金 12 ヶ月分に限定されるという条件は、しばしばみられることであった。だが、前述のとおり、従来第三者に渡して処理してもらう個人データの漏えい時の損害と比較すると、OpenAI 社の AI サービスを用いて処理させる個人データの漏えいリスクや漏えい時の損害は、相当程度大きい。ところが、OpenAI 社の AI サービスの約款では、そのような大きな危険に比例するだけの大きな責任は、同社はわずか 12 ヶ月分の代金を超えては負わないと宣言している。この点は、多くのユーザー企業のリスク想定を超えているのではないか。

ユーザー企業側は、AI を用いて OpenAI 社に個人データを分析させる場合は、自ら相当の多額の IT 保険に入るなどして、OpenAI 社の過失で分析対象の個人データが漏えいした場合の個人からの損害賠償請求に備えておく必要があるそうである。

133
134 なお、いかなるソフトウェアにも、脆弱性と呼ばれる欠陥が存在する。OpenAI 社
135 の AI システムは高度かつ大規模であり、同社が開発運用するソフトウェアの欠
136 陥だけでなく、それらのソフトウェアが動作する下位のクラウド基盤・GPU 基盤
137 や、ストレージ基盤、ネットワークの暗号化処理基盤、ユーザー認証基盤などの
138 さまざまなコンポーネントが密接に関連して動作しているが（※ 2）、これらのう
139 ちわずか 1 個の中の 1 箇所にでも脆弱性があれば、そこからデータが漏えいし
140 得る。OpenAI 社は、これらの他の多数のクラウド事業者の基盤を、内部的に利用
141 している。従来型のデータ処理受託者のシステムと比較して、非常に複雑な構造
142 となっており、リスクも高い。だが、いずれの部分がセキュリティ侵害されても、
143 ユーザー企業が OpenAI 社から賠償を受けることができるのは直近代金の 12 ヶ
144 月分にとどまるのである。

- 146 (3) OpenAI 企業向け約款 13 節をよく読むと、OpenAI 社に対して、ユーザー企業は、
147 原則として、裁判所に対して民事訴訟を起こせないようになっている（義務的仲
148 裁の規定）。日本の裁判所はもちろんのこと、米国の裁判所に対しても訴えること
149 が禁止されている。その代わりに、OpenAI 社が一方的に希望する合意仲裁人とし
150 て、米国ニューヨーク州の営利企業である「NAM 社」という会社が指名されてい
151 る。日本のユーザー企業は、公正な裁判所を利用する代わりに、営利企業 NAM 社
152 のお裁きを受けることに、予め同意させられるようになっている。

153 たしかに、米国では、仲裁（ADR）が普及している。米国の裁判においては、裁判
154 所が審理に入る前に、当事者に対して、まず仲裁によって解決を試行するよう指
155 示するケースが多いと聞く。しかしながら、その場合は、仲裁結果に不満足であれ
156 ば、いずれかの当事者は、改めて裁判所に審理してもらうことができる。ところが、
157 この OpenAI 社の約款における義務的仲裁の事前同意の規定は、これと異なり、
158 当事者がたとえ仲裁結果に不満足であっても、公平な裁判所の審理を受ける
159 ことを予め禁止する（日本のユーザー企業は、公平な裁判を受ける権利を予め放
160 棄させられる）という仕組みになっている。

161 そもそも、一般的な日本企業で外国の私企業による仲裁（ADR）を経験したものは
162 少ないだろうし、知見のある弁護士も多いとは思われない。外国での訟務は大手
163 渉外弁護士事務所の、かつ米国における国際仲裁合意に関する実務に精通した弁
164 護士（人数に限られる）を頼ることが多いだろうが、そのような大手事務所や前
165 記実務に精通した弁護士はもともと OpenAI 社あるいは OpenAI 社の筆頭株主か
166 つ事業パートナーの外資企業（例えば、マイクロソフト社）からの仕事をもらっ
167 ている場合も多くなると考えられ、紛争発生時にユーザー企業側の頼る先がない
168 といったことにもなりかねない。すると、仮に OpenAI 社が原因で、本文書で想
169 定・指摘しているような問題が原因で、個人データの漏えいや目的外利用がなされ
170 した場合、日本のユーザー企業が同社に損害賠償を求めたくても、絵に描いた餅
171 になりかねない。これらは、日本企業の通常の視点を想定すると、おおいに気にな
172 る点である。

- 174 (4) 約款に、「顧客の権利または義務に重大な影響を及ぼすと弊社（OpenAI 社）が独
175 自裁量で判断した場合」であっても、30 日前の通知で、一方的に約款変更できる、
176 とある（→ OpenAI 企業向け約款 14.1 節）。仮に、OpenAI 社が、企業が入力す

る個人データ等に関する保護義務等を緩和・撤廃したいと思ったでしょう。これは、「顧客の権利に重大な影響を及ぼす」事柄であり、日本の民法の定型約款の変更の規定（民法 548 条の 4）によれば、勝手に変更できないはずである。だが、準拠法が米国カリフォルニア州法なので（→ OpenAI 企業向け約款 15.2 節）、日本の民法の定型約款における規制が適用されない。すると、同社は 30 日前に通知するだけで、そのような約款変更ができてしまうのではないかと、という点が気になる。

(5) OpenAI 社は、いつでも本約款の契約上の地位を「関連会社」に移転できるとあるが、「関連会社」の定義がないように見える（→ OpenAI 企業向け約款 15.9 節）。米国における「関連会社」という用語の用法を用いるとすれば、米国証券取引委員会（SEC）の基準によると、「関連会社」とは約 10% 以上の資本関係がある企業という意味で、かなり広い。このような極めて幅広い第三者に、OpenAI 社は、日本企業の同意なく、いつでも、事業譲渡できてしまう。すると、譲渡先の第三者に、個人情報引き渡されるリスクがある。OpenAI 社は、この仕組みを用いて、同社に蓄積した日本企業の大量の個人データのうち、全部または特に市場価値の高い一部分を切り出して、有償で他社に売却できてしまうのではないかと。

(6) 本約款およびプライバシーポリシーにおいては、法律上の義務を遵守するため（→ OpenAI Privacy policy 2 節, 4 節およびデータ処理委託特約 2 節）に、個人データを目的外で保存あるいは開示できるという規定がある。だが、契約に係る裁判管轄は米国カリフォルニア州サンフランシスコ郡の連邦裁判所または州立裁判所、裁判地は同州、準拠法は同州法となっているから、ここでいう「法律」とは、カリフォルニア州法を指すと思われる。通常の日本企業は、カリフォルニア州法になじみがないだろうから、こういった場合に上記記述が適用されるのか不明であり、また契約上の紛議が発生したら、カリフォルニア州法の解釈適用が争われることになり、その場合、日本企業としては太刀打ちできないのではないかと。

(7) ChatGPT には、ユーザーデータが学習に利用されないようにする設定がある。だが、プライバシーポリシーをよく読むと、単にモデル学習に利用されなくなるだけでなく、その他の目的で収集され利用される旨の記載がある（→ OpenAI Privacy policy 2 節）。また、米国カリフォルニア州法あるいは米国法が要求する場合は、OpenAI 社から第三者に開示することができる、と規定されている（→ OpenAI Privacy policy 3 節）、（→ データ処理委託特約 2 節）。他方で、OpenAI を利用して個人データを処理させようとするユーザー企業の側は、日本の個人情報保護法に従う必要があるが、日本の個人情報保護法 27 条 1 項 1 号における「法令に基づく場合」の「法令」とは、㊦ 日本国の法令のみを示すのか、それとも、㊩ 当該外国委託先企業の存する外国の法令も含むのかが、問題となる。これについて、日本政府は、国会答弁で ㊦ であるとの公式見解を出している（2019 年 6 月 25 日衆議院答弁第 227 号）。この日本政府の公式見解に従う限り、日本の個人情報保護法によれば、仮に OpenAI 社がデータ処理の委託先として日本の個人情報保護法を遵守するのであれば、たとえ米国カリフォルニア州法あるいは米国法が要求する場合であっても、日本の法令が要求しない限り、OpenAI 社はユーザ

データを第三者（たとえば、米国捜査機関等）に開示することはできないはずである。だが、約款には上記のとおり「できる」とあるので、これは日本の個人情報保護法の考え方と矛盾しているように見える。

また、OpenAI 社は、入力された個人データを「① 当社の顧客たち、② 当社自身および ③ 第三者の法的権利、プライバシー権利、安全および財産を保安するため」に顧客の承諾無く勝手に「使用」（その文言から、第三者への提供を含むと思われる）することができると規定されている。仮に OpenAI 社がデータ処理の委託先として日本の個人情報保護法を遵守するのであれば、日本の個人情報保護法 27 条 1 項 2 号の「人の生命、身体又は財産の保護のために必要がある場合であって、『④ 本人の同意を得ることが困難であるとき。』」という条件にあてはまらない限り、同目的では個人データを勝手に「使用」（第三者への提供）することはできないはずである。特に日本の個人情報保護法では ④ の本人同意取得困難性の要件が規定されているが、OpenAI 社の規定には、それが無い。これは、日本の個人情報保護法の考え方と矛盾しているように見える。

- (8) 「個人情報の（第三者への）開示」という節で、包括承継だけでなく単なる任意の事業譲渡契約の場合だけでも、さらには、事業譲渡を予定している相手方からの資産状態把握プロセスで要求された場合でも、OpenAI 社は、個人情報を「第三者」に開示できると規定されている（→ OpenAI Privacy policy 3 節）。たしかに、日本の個人情報保護法にも、事業の承継の際を想定し例外的に第三者提供を認める類似の規定がある（27 条 5 項 2 号）。個人情報保護委員会のガイドライン通則編 3-6-3 には、「事業の承継のための契約を締結するより前の交渉段階で、相手会社から自社の調査を受け、自社の個人データを相手会社へ提供する場合も、本号に該当し、あらかじめ本人の同意を得ることなく又は第三者提供におけるオプトアウト手続を行うことなく、個人データを提供することができる」とある。だが、同ガイドラインには、続いて、「当該データの利用目的及び取扱方法、漏えい等が発生した場合の措置、事業承継の交渉が不調となった場合の措置等、相手会社に安全管理措置を遵守させるために必要な契約を締結しなければならない。」・・・ ① という安全策を施す義務が規定されている。

https://www.ppc.go.jp/personalinfo/legal/guidelines_tsusoku/#a3-6-3

これと比較して、OpenAI 社のプライバシーポリシーでは、事業譲渡の予定がある場合における個人データを提供について、① のような安全策を施す義務の規定がない。すなわち、事業譲渡を予定するとして第三者にデータを提供したのち、交渉が不調に終わったとしても、その第三者にデータを確実に削除させる等を義務付ける契約を締結する旨の規定がない。すると、OpenAI 社は、このスキームを形式的に用いることで、任意の第三者に個人情報を渡してしまうことができるのではないかという点が気になる。

- (9) OpenAI 社は、法令（米国カリフォルニア州法および米国法）に基づき、「同業他社、あるいはその他の第三者」に対して個人情報を開示できると記載されている（→ OpenAI Privacy policy 3 節）。しかも、法令によって強制された場合だけでなく、OpenAI 社が「法律上の義務を履行するために必要であると誠実に信じる場合」にも、第三者に個人情報を開示できると記載されている。これは相当の裁量を OpenAI 社に委ねる規定になっている。OpenAI 社が「必要であると誠実に信じ

る場合」であれば、個人情報情報を第三者に渡してしまえることになる。実際にはそれが必要でなかったことが後から判明しても、渡してしまった情報を回収し、または削除させることを担保する規定がなく、一度侵害された個人情報にかかる秘匿性という権利利益を回復することが困難な規定になっている。

(10) 受け取った個人データを、サービスを提供するために必要な期間のほか、OpenAI 社の適法なビジネス上の目的（法的紛争、安全や保安上の理由、他に法的に義務付けられる規制に適合することを含む）で必要な限り保持し続けることができる」と規定されている（OpenAI Privacy policy 4）。つまり、顧客にとって無関係あるいは不利益な場合でも、OpenAI 社の利益のためだけに、顧客の意思に反し、個人データが合法的に保持されてしまう（削除してもらえない）のではないかという点が気になる。

(11) プライバシーポリシーは、「別途適用される法律で要求されない限り」いつでも変更できると記載されている（→ OpenAI Privacy policy 9 節）。「別途適用される法律」とは、約款で定められているとおり、準拠法、すなわち米国カリフォルニア州法および米国法であり、日本の民法の定型約款の変更に掛かる規制（民法 548 条の 4）の適用は彼らの認識対象外であるおそれがあり、日本の個人情報保護法もまた、彼らの認識対象外であるおそれがある。仮に、あるときは個人データの処理に OpenAI を利用しているユーザー企業側の利用方法が個人情報保護法に適合していたとしても、OpenAI 社によって一方的にプライバシーポリシーが変更された途端、突然、個人情報保護法に違反してしまう問題が発生するのではないかという点が気になる。

(12) 「ビジネスデータ」（ChatGPT や OpenAI API の入出力プロンプトデータ）の内容について、「当社サービスの利用法に対する理解を深めることなど」（原文のまま）という目的で、自動分類し、かつ、「人間によって」そのデータの検証がなされる、と明記されている（→ OpenAI における企業プライバシー 「サービス全般」の「Q. OpenAI は顧客のビジネスデータの検証を行いますか？」）。つまり、OpenAI 社は、「当社サービスの利用法に対する理解を深めることなど」を目的として、OpenAI 社の従業員によって、目視し、分析することができるということになる。

すると、個人情報保護委員会の「生成 AI サービスの利用に関する注意喚起等令和 5 年 6 月 2 日」の「(1) ②」の「当該個人データが当該プロンプトに対する応答結果の出力以外の目的で取り扱われる場合」に該当してしまうのではないか。

この状態で、日本企業が個人データを入力すると、事前の個人本人の同意を得ない限り、個人情報保護法に違反することになってしまわないか？という点が気になる。

(13) 上記の「気になる点」は、OpenAI 社のサービスを直接契約して利用する場合だけの問題ではない。AI サービスやデータ処理サービスの中には、OpenAI 社の API を内部的に呼び出して処理をしているものがあり、その数は増加し続けられると思われる。そういった、内部的に OpenAI の API サービスを呼び出しているす

309 べての応用サービスを利用して、個人データあるいは営業機密を処理したいと考
310 えている、すべての日本企業のユースケースで、上記が問題になるのではないだ
311 ろうか。

312 つまり、A が、B という日本企業が提供するサービス C を利用するとして、C
313 は直接または間接的に OpenAI 社の API を呼び出して、A の入力する個人デー
314 タを GPT で処理しているとする。A は B としか契約していないが、そこで入力
315 される個人データは、契約関係のない OpenAI 社によって AI 処理される。この
316 際、B と OpenAI 社との間の契約関係上生じる上記で述べたような問題のほとん
317 どが、A に対しても発生する。それによって、A が各個人本人に対して責任を負
318 う個人情報保護法の義務（たとえば、事前の本人からの同意取得義務）の内容が
319 左右されてしまう。また、A は、B に対する監督責任の一部として、OpenAI 社
320 に対する監督責任も発生してしまう。どのようにそれを完遂するのか。このよう
321 なトランジット的な A サービス呼び出し関係を考えると、OpenAI 社の企業向け
322 約款に上記のような気になる点がある場合、その影響範囲は、極めて広いものに
323 ならないだろうか。

324
325 3. 上記の各項目について、OpenAI 社の企業向け約款等（英語の部分の日本語訳は、
326 当方が自分で訳した参考訳です。間違っていたらすみません。）とともに、下記で、
327 もう少し詳しく述べます。

328
329 4. この検討会の他の委員の先生方の皆様は、法学者や弁護士の方々です。それと比べ
330 て、私は、法律については素人で、知識はほとんどありません。この内容は、私が、
331 一般的企業の AI サービスを利用したいと思う担当者の視点で、既存の AI サービ
332 スの約款を読んで気になった点を列挙するものです。自分の素人的な視点は、普通
333 の企業の普通の担当者がちょっと約款等を読んだならば気にするだろうという点を
334 挙げるためには、便利なものだと思っています。専門家の読者の方々からみて、実
335 は法律的にはこの点は全く心配がないから懸念しなくても大丈夫、というような内
336 容も、色々含まれているかも知れません。そのような間違いがありましたら、い
337 つでも、ぜひ教えていただければ幸いです。連絡先メールアドレスは、上部に記載
338 してあります。間違いを教えていただきましたら、本文書の内容をすみやかに訂正
339 したいと思います。

342 ■ 第一. 『OpenAI Business terms (OpenAI 企業向け約款) November 14, 2023』に 343 ついて

344
345 『OpenAI Business terms (OpenAI 企業向け約款) November 14, 2023』

346 原文: <https://openai.com/policies/business-terms/>

347
348 6. Privacy

349 6. プライバシー

350
351 6.1 Personal Data. If you use the Services to process personal data, you must
352 (a) provide legally adequate privacy notices and obtain necessary

consents for the processing of personal data by the Services, (b) process personal data in accordance with applicable law, and (c) if processing "personal data" or "Personal Information" as defined under applicable data protection laws, execute our Data Processing Addendum by filling out this form (opens in a new window).

6.1 個人データ。顧客が本サービスを個人データを取り扱うために利用する場合は、顧客は、(a) 法律上適切なプライバシーに関する通知を行ない、本サービスで個人データを取り扱うために必要な同意を取得しなければなりません。(b) 適用される法令に従って個人データを取り扱わなければなりません。(c) 適用される個人情報保護法のもとで定義される「個人データ」あるいは「個人情報」を取り扱う場合においては、当社との間で、DPA（データ処理委託特約。編注：EU の顧客は GDPR に基づいて締結が要求されているものと思われる）を、このフォーム（編注：リンクが貼ってある）を用いて締結しなければなりません。

⇒ OpenAI 社は、GPT サービスを用いて顧客が個人データを取り扱う ("process personal data") 場合を想定し、顧客に対して、(a) 関係法令に基づき、個人から同意を取得しなければならない旨、(b) 関係法令を遵守しなければならない旨、(c) EU の GDPR 規制を想定し、EU の顧客との間では DPA (GDPR で要求されるデータ処理委託特約) を個別締結しなければならない旨、の 3 点を、この約款で宣明している。

⇒ このことから、OpenAI 社は、少なくとも、プロンプトを介して処理を依頼される個人データを扱う場合、これを「委託を受けたもの」として扱っているといえるのではないかと。(なお、後述の「OpenAI Privacy policy」では、さらに踏み込んで、*"We collect Personal Data that you provide in the input to our Services"* (参考訳: 「当社は、顧客が当社のサービスに対して入力した個人データを収集する」) とも記載されている。)

⇒ そして、この「OpenAI 企業向け約款」に基づいて、顧客と OpenAI 社との契約が締結されることから、個人データを OpenAI 社が取り扱う旨の双方の意思の一致があるので、それが契約の内容となることになる。すると、日本企業と OpenAI 社との間で成立した契約上は、個人情報委員会といういわゆるクラウド例外の規定が適用される余地はないのではないかと。

11. Limitation of Liability

11. 損害賠償の制限

11.2 Liability Cap. Except for (i) a party's gross negligence or willful misconduct or (ii) a party's indemnification obligations under this Agreement, each party's total liability under the Agreement will not exceed the total amount you have paid to us in the twelve (12) months immediately prior to the event giving rise to liability. The foregoing limitations will apply despite any failure of essential purpose of any limited remedy and to the maximum extent permitted under applicable law.

11.2 賠償の上限額。(i) 当事者の重過失あるいは故意、(ii) 本契約で補償義務が規定されている場合をのぞき、いずれの当事者も、損害賠償債務を生じせしめる事

象に先立つ 12 ヶ月間に顧客が当社に対して支払った総額を超えて賠償義務を負わないものとします。この制限は、制限的な救済手段が本質的目的を果たせない場合にも適用され、また、適用される法律で認められる最大限の範囲で適用されるものとします。

⇒ OpenAI 社が個人データや営業秘密を扱う場合に、OpenAI 社のクラウド基盤がサイバー攻撃者によって攻撃され、各利用企業のすべての過去プロンプト入力データ（学習しない設定になっていても、彼らのいう「法令遵守」のために記録されている可能性がある。プライバシーポリシー参照）が全部流出するリスクがある。この場合、利用企業は莫大な損害を受けるが（守秘義務を負う個人あるいは取引先に対して賠償しなければならないため）、たとえ原因が OpenAI 社によるシステムソフトウェア上の過失であっても、利用企業は、彼らの「重過失」を証明できない限り、わずか「12 ヶ月分」の賠償しか受けられない。そして、「重過失」の証明のハードルは、相当高い。OpenAI のデータセンタのサーバー内のプログラムコードや設定、プログラムの当時の会話ログ等を分析しなければならない。隠ぺいされると思われるので、この責任追及は、事実上不可能であるのではないか。

⇒ 多数の日本企業や日本の個人は、いわゆる泣き寝入りを強いられることになるのではないか。

⇒ この点について、IT 法務に詳しいある弁護士に個人的に有償で相談したところ、「その通りです。実際、オンラインゲームのクラウドサーバが停止等して膨大な損害が出ても、重過失が証明できて補填できたという話は聞いたことはありません。障害自体はしばしば起きています。例えば、以下 URL」との回答があった。

「AWS で 1 時間強にわたり障害、PayPay や一部アプリが一時利用できず」

<https://xtech.nikkei.com/atcl/nxt/news/18/09003/>

13. Dispute Resolution

13. 紛争の解決

YOU AGREE TO THE FOLLOWING MANDATORY ARBITRATION AND CLASS ACTION WAIVER PROVISIONS:

顧客は、以下の義務的仲裁および集団訴訟放棄規定に同意するものとします:

13.1 MANDATORY ARBITRATION. You and OpenAI agree to resolve any claims arising out of or relating to this Agreement or our Services, regardless of when the claim arose, even if it was before this Agreement existed (a "Dispute"), through final and binding arbitration.

13.1 義務的仲裁。ユーザーと OpenAI は、本契約に起因する、または本契約もしくは当社サービスに関連するあらゆる請求（以下、「紛争」といいます）を、その請求がいつ発生したかにかかわらず、たとえ本契約が存在する以前であっても、最終的かつ拘束力のある仲裁を通じて解決することに同意するものとします。

- ⇒ これは大変に深刻な規定である。この規定が存在することで、仲裁合意があったとみなされてしまい、通常の訴訟（日本国の裁判所の訴訟であっても、米国の裁判所の訴訟であっても）が利用できないことになってしまう。準拠法および合意された仲裁地が米国カリフォルニア州（後述）とされていることから、日本の仲裁法 44 条の規定が利用できず、日本の裁判所に、仲裁の取消しを申立てることもできない（基本書「国際関係私法入門」（第 4 版補訂）松岡博 第 19 章「仲裁」参照）。
- ⇒ たしかに、米国の裁判においては、裁判所が審理に入る前に、当事者に対して、まず仲裁によって解決を試行するよう指示するケースが多いと聞く。しかしながら、その場合は、仲裁結果に不満足であればいずれかの当事者は改めて裁判所に審理してもらうことができるはずである。この OpenAI 社の約款における義務的仲裁の規定は、これと異なり、当事者がたとえ仲裁結果に不満足であっても、公平な裁判所の審理を受けることを予め禁止する（日本のユーザー企業は、公平な裁判を受ける権利を予め放棄させられる）という仕組みになっている。
- ⇒ 日本企業で外国の私企業による仲裁（ADR）を経験したものは少ないだろうし、知見のある弁護士も多いとは思われない。外国での訟務は大手渉外弁護士事務所の、かつ米国における国際仲裁合意に関する実務に精通した弁護士（人数が限られる）を頼ることが多いだろうが、そのような大手事務所や前記実務に精通した弁護士はもともと OpenAI 社あるいはマイクロソフト社（OpenAI 社の筆頭株主かつ事業パートナー）からの仕事をもらっている場合も多くなると考えられ、紛争発生時にユーザー企業の頼る先がないといったことにもなりかねない。ほとんどの場合、ユーザーである日本企業は、圧倒的に不利な立場に立たされるのではないか。
- ⇒ これまで、日本企業は、たいていデータ処理を他の日本企業（あるいは、日本に設立された外資系の企業）に委託してきた。ところが、OpenAI 社にはそのようなオプションがない。そして、国際仲裁合意を強制してくるのである。このような経営上の重大なリスクに気付かずに契約を締結してしまう日本企業経営者は多いため、仲裁の場合のデメリット、仲裁地および準拠法が外国である場合のデメリット等を、適切に注意喚起する必要があるのではないか。
- ⇒ この点について、IT 法務に詳しいある弁護士に個人的に有償で相談したところ、「米国での仲裁が現実的にペイするような API 利用者はほとんどいないと思います。事実上、泣き寝入りです。」との回答があった。

13.3 Arbitration Forum. Both you or OpenAI may commence binding arbitration through National Arbitration and Mediation (NAM), an alternative dispute resolution provider, and if NAM is not available, you and OpenAI will select an alternative arbitral forum. The initiating party must pay all filing fees for the arbitration and payment for other administrative and arbitrator's costs will be governed by the arbitration provider's rules. If your claim is determined to be frivolous, you are responsible for reimbursing us for all administrative, hearing, and other fees that we have incurred as a result of the frivolous claim.

13.3 仲裁機関。顧客または OpenAI の双方は、紛争仲裁機関である「National Arbitration and Mediation 社」（NAM 社。編注：米国のニューヨーク州にある

仲裁サービスを提供する LLC = 営利企業) を通じて、法的拘束力のある仲裁を開始することができます。NAM 社が利用できない場合は、顧客と OpenAI は、代替りの仲裁機関を選択するものとします。仲裁を開始する当事者の側が、仲裁の申立手数料をすべて支払わなければならない、その他の管理費および仲裁人の費用の支払いは、仲裁機関の規則に準拠します。顧客の請求が一見明白に理由がないものと判断された場合、顧客は、かかる一看明白に理由のない請求の結果として当社が負担したすべての管理費、審理費、およびその他の費用を当社に返還しなければなりません。

⇒ 仲裁機関として、原則として、米国ニューヨーク州の営利企業である NAM 社のみを利用することを強いる規定である。その他の仲裁機関の選択は、NAM 社が利用できない場合に限る、とされている。

⇒ ここで、日本の経営者からみた問題は、次のとおりであると思われる。(a) 利用が強制させられる「NAM 社」に中立性があることを、日本企業の立場からみて、どのように担保するのかという点。NAM 社は出資者や議決権の保有者やその比率が非公開な私企業であり、日本企業として、NAM 社の中立性をどのように検証すれば良いのか不明確である。(b) NAM 社は米国の私人が仲裁判断をする米国企業であり、一般的な予測として、米国企業にとって有利な判断をしてしまうリスクが高いのではないかと。いう点。(c) NAM 社という私人の裁定により結果が確定したら、正規の裁判所に上訴することができないのではないかと。いう点。

13.4 Arbitration Procedures. The arbitration will be conducted by telephone, based on written submissions, video conference, or in person in San Francisco, California or at another mutually agreed location. The arbitration will be conducted by a sole arbitrator by NAM under its then-prevailing rules. All issues are for the arbitrator to decide, except a California court has the authority to determine (a) whether any provision of this arbitration agreement should be severed and the consequences of said severance, (b) whether you have complied with conditions precedent to arbitration, and (c) whether an arbitration provider is available to hear the arbitration (s) under Section 13.3. The amount of any settlement offer will not be disclosed to the arbitrator by either party until after the arbitrator determines the final award, if any.

13.4 仲裁手続き。仲裁は、準備書面の事前提出に基づく、電話会議、ビデオ会議、または米国カリフォルニア州サンフランシスコ（相互に合意した場合は、別の場所でも可）での直接面談により行われます。仲裁は、その時点で有効な規則に基づき、NAM 社による単独の仲裁人によって行われます。(a) 本仲裁合意のいずれかの条項が分離されるべきかどうか、および当該分離の結果、(b) 顧客が仲裁に先行する条件を遵守したかどうか、および (c) 13.3 に基づき仲裁の提供事業者が仲裁の管轄権を有するかどうかを判断する権限を米国カリフォルニア州裁判所が有する場合を除き、すべての問題は仲裁人が決定するものとします。和解案の金額は、仲裁人が最終裁定（もしあれば）を決定するまで、いずれの当事者も仲裁人に開示しないものとします。

⇒ 日本企業側が NAM 社に仲裁管轄権がないと考えた場合でも、本仲裁合意によれば、その仲裁管轄権の有無の判断権限は、米国カリフォルニア州裁判所にあるとされ、日本の裁判所にはないとされている点が問題ではないか。

14. Modifications to these Business Terms and the OpenAI Policies

14. 本約款および OpenAI ポリシーの変更

14.1 Updates. We may update these Business Terms or the OpenAI Policies by providing you with reasonable notice, including by posting the update on our website. If, in our sole judgment, an update materially impacts your rights or obligations, we will provide at least 30 days' notice before the update goes into effect, unless the update is necessary for us to comply with applicable law, in which case we will provide you with as much notice as reasonably possible. Any other updates will be effective on the date we post the updated Business Terms or OpenAI Policies. Your continued use of, or access to, the Services after an update goes into effect will constitute acceptance of the update. If you do not agree with an update, you may stop using the Services or terminate this Agreement under Section 8.2 (Termination).

14.1 更新。当社は、当社ウェブサイトへの掲載を含め、合理的な通知を顧客に行なうことにより、本約款または OpenAI ポリシーを更新することができます。更新が顧客の権利または義務に重大な影響を及ぼすと弊社が独自裁量で判断した場合、弊社は、更新が適用される法律を遵守するために必要な場合を除き、更新が発効する少なくとも 30 日前に通知を行います。その他の更新は、当社が更新されたビジネス規約または OpenAI ポリシーを掲載した日に発効するものとします。更新の発効後、顧客が本サービスの継続的な使用または本サービスへのアクセスを行った場合、更新に同意したものとみなされます。顧客が変更に同意されない場合、本サービスの利用を停止するか、または 8.2（解約）に基づき本契約を解約することができます。

⇒ 約款が「顧客の権利または義務に重大な影響を及ぼすと弊社が独自裁量で判断した場合」であっても、30 日前の通知で、一方的に変更できる、とある。

⇒ このように、顧客が一方的に重大な不利益を被る場合は、少なくとも日本法では、民法 548 条の 4（定型約款の変更）第 1 条 1 号にも 2 号にも、該当しないので、定型約款の変更として有効に認められないのではないかと考える。

⇒ ところが、後述のとおり、顧客と OpenAI との契約の準拠法が米国カリフォルニア州法であると約款に定められているので、企業経営者は、米国カリフォルニア州法を勉強した上で、約款「14.1」に基づく約款の大幅な不利益変更が有効となるか否かを、事前に判断しなければならないことになる。

⇒ 仮に、米国カリフォルニア州法に基づくそのような約款変更が有効である可能性がある、としよう。この場合、OpenAI が個人データを一定程度機密に保管する（後述のとおり、プライバシーポリシー上は、かなり不十分であるが）義務が約款上規定されていても、OpenAI 社は、30 日前の通知で、突然その保護レベル

をさらに低下させることもできてしまう、ということになる。そうすると、日本企業は、仮に低下前であれば個人情報保護法上のリスクが受忍限度内である判断していた場合でも、低下後であれば受忍限度を超えると判断した場合、直ちに OpenAI 社のサービスを利用停止しなければならない。前述のとおり、日本の民法 548 条の 4 に従う約款変更であれば、そのようなことが突然発生するリスクはとても小さい。だが、米国カリフォルニア州法準拠であれば、そうもいかない。このことは、日本企業にとって大きな経営上の打撃となる。

⇒ さらに、更新が顧客の権利または義務に重大な影響を及ぼすと弊社が「独自裁量で判断した場合」の「独自裁量」(in our sole judgment) という部分が、日本企業にとって、極めて大きな懸念点となる。日本企業は、この OpenAI 社の独自裁量権に服さなければならないのか。そうだとすれば、OpenAI 社は「独自裁量」で、少し個人データのセキュリティ保護機構を引き下げることが「重大な影響」を及ぼすものではないと判断した上で、30 日の前置通知をせずに、突然に約款を変更できてしまうことになる。繰り返しであるが、その約款の変更の有効性は、日本国民法ではなく、米国カリフォルニア州法で、かつ米国カリフォルニア州裁判所によって判断されてしまうのである。

⇒ これらを総合して考えると、次のことがいえる。日本企業の経営者は、OpenAI 社と契約した上で個人データを AI 処理する場合、安全管理措置あるいは委託にかかる相当措置を講ずるためには、少なくとも、(a) 約款群を全部読んだ上で、(b) 米国カリフォルニア州法の判例体系も勉強し、(c) 個人情報保護に関わるセキュリティ上の義務を緩和する形で約款が突然変更されてしまうことの米国カリフォルニア州法上の有効性の有無を検討し、(d) それらを総合して法的に大丈夫であるという結論を導出しなければ、同目的で OpenAI を利用することができない。これらの事柄をきちんと監理せずに個人データを OpenAI に投入することは安全措置義務等を履行していないとみなされ得る。だが、それができる日本企業経営者はどこまでいるのか。個別に弁護士に相談して判断してもらえるのだろうか。おそらく無理なのではないか [※ 3]。そうすると、一般的な外国 AI 企業と約款契約を締結する場合における上記の観点を含んだ考え方や注意点を十分にわかりやすく提示する判断材料を、本件 AI チェックリストに含めることは、日本企業が AI を利用することを想定して不可欠の仕事なのではないか。

⇒ ※ 3. この点について、IT 法務に詳しいある個人的に有償で相談したところ、「まあほぼ無理でしょうね。」との回答があった。

15. Miscellaneous

15. 細則

15.9 Assignment. This Agreement cannot be assigned other than as permitted under this Section 15.9 (Assignment). We may assign this Agreement to an affiliate without notice or your consent. Both you and OpenAI may assign this Agreement to a successor to substantially all the respective party's assets or business, provided that the assigning party provides reasonable (at least 30 days) prior written notice of the assignment. This Agreement will be binding upon the parties and their respective successors and permitted assigns.

15.9 譲渡。(略) 当社は、通知やお客様の同意なしに、本契約を関連会社 (an affiliate) に譲渡することができます。(略)

⇒ "affiliate" とは、「関係会社」という意味である。だが、本約款には「関係会社」の用語の定義がなく曖昧である。

⇒ (1) そこで、米国証券取引委員会 (SEC) の示している基準が参考になる。米国証券取引委員会は、2017 年の上場企業へのレターによると、「関係会社」の基準を、おおむね発行済株式総数の約 10% 以上の資本関係があるものであると解釈している。これは、かなり緩い基準である。

<https://www.sec.gov/Archives/edgar/data/1585608/000110465917056773/>

(↑ 上記の URL が改行されている場合は、改行をつなぎ合わせてアクセスする必要がある場合があります。)

⇒ (2) あるいは、『OpenAI Privacy policy November 4, 2024 版』(企業向け API アクセスの場合は適用除外) には、3 条 1 項で「関連会社: 当社は、個人データを当社の関連会社 (OpenAI を支配する事業体、OpenAI によって支配される事業体、又は OpenAI と共通の支配下にある事業体を意味します) に開示することがあります。当社の関連会社は、本プライバシーポリシーに従った方法により、この個人データを使用することがあります。」と記載されている。OpenAI としては、この認識である可能性もある。

⇒ いずれにしても、非常に広い範囲の任意の第三者を指して、「関係会社」であると主張できてしまう仕組みになっているように見える。

⇒ この約款の上記部分によると、OpenAI 社は、いつでも本約款の契約上の地位を「関連会社」に移転できることになる。関連会社の基準を満たささえすれば、契約上の地位 (特に、個人データを顧客である日本企業のために適切に保護するという債務者としての地位) が OpenAI 社以外の第三者に、事前通知あるいは同意 (without notice or your consent) なしに、突然に移転されてしまうことに、予め顧客である日本企業が同意させられていることになる。

⇒ 個人情報保護法上の問題として、次のような事態が容易に発生する。企業は安全管理措置あるいは相当措置を OpenAI 社に対して行ってきたことにより法律を遵守していたところ、OpenAI 社から、わずか 10% 程度の株式関係があるに過ぎない他の第三者に「事前通知あるいは同意 (without notice or your consent) なし」に契約上の地位が移転されてしまうリスクを負うことになる。だが、安全管理措置あるいは相当措置は、相手方企業である OpenAI 社との個別の信頼関係に基づき具備される必要がある措置である。ここで、突然に事前通知なく OpenAI 社が他社に地位を譲渡してしまうことを日本企業側が承諾してしまうと、そのような安全措置を継続維持することは事実上不可能になってしまう。

15.12 Jurisdiction, Venue, and Choice of Law. This Agreement will be governed by the laws of the State of California, excluding California's conflicts of law rules or principles. Except as provided in the Section 13 (Dispute Resolution), all claims arising out of or relating to this Agreement will be brought exclusively in the federal or state courts of

San Francisco County, California, USA.

15.12 裁判管轄、裁判地および準拠法。本契約は、米国カリフォルニア州法の抵触法に関する規則または原則に反しない限り、米国カリフォルニア州法に準拠するものとします。13（紛争解決）に規定されている場合を除き、本契約に起因または関連するすべての請求は、専属的に、米国カリフォルニア州サンフランシスコ郡の連邦裁判所または州裁判所に提起されるものとします。

- ⇒ 契約に係る裁判管轄は米国カリフォルニア州サンフランシスコ郡の連邦裁判所または州立裁判所、裁判地は同州、準拠法は同州法であることに、日本企業は同意させられることになる。
- ⇒ この場合、次の問題が発生する。本約款およびプライバシーポリシーにおいて、法令遵守の記述がある（特に個人データの扱いの点）。日本企業としては、これらの法令とは、日本の個人情報保護法を意味しているので、OpenAI 社は日本の個人情報保護法を遵守してくれるのであろう、と誤信してしまうことは、ほとんど確実である。だが、OpenAI は、次のように否認するであろう。すなわち、15.2 の規定により準拠法は米国カリフォルニア州法であるとされているし、6.1 (c) にあるような EU 向けのデータ処理委託特約 (DPA) も締結されていないのだから、OpenAI は日本の個人情報保護法など遵守する必要はないはずである、と述べるであろう。そして、それは米国カリフォルニア州サンフランシスコ郡の連邦裁判所に通用してしまう可能性がある。少なくとも日本企業と OpenAI 社との係争を行なう審判者である民間企業 NAM 社による ADR（仲裁、約款 13 節参照）上においては審判者はそのように判断するであろう（そして、前述のとおり、外国仲裁地の合意があるので、仲裁法 44 条に基づく裁判所への訴えは却下されてしまう）。
- ⇒ すると、本約款やプライバシーポリシーにおいては、日本企業との契約上の関係においては、OpenAI 社は日本の個人情報保護法その他の法令を遵守する義務がないことになってしまうリスクがあり [※ 4]、日本の個人情報保護法が要求する相当な安全措置を講ずる必要が OpenAI 社の契約上の債務として発生しないことになる。この場合、OpenAI 社のサービスを用いて個人データを処理してしまうと、利用企業側が日本の個人情報保護法に違反することになる高いリスクが生じる。
- ⇒ ※ 4. 日本の個人情報保護法 171 条には、域外適用の規定があるから、日本の主権者の立場としては、同法は、外国でも通用する。だが、日本の法律というものは、単に日本の主権者が定めた法であり、外国で外国の裁判主体に対して通用するかどうかは別問題である。法的問題が発生した時に、その外国の裁判所あるいは仲裁人が、適用される法のもとで、日本の個人情報保護法の規定も OpenAI 社を拘束すると判断してくれる保証はない。
- ⇒ 日本の利用企業側が OpenAI 社サービスを利用する場合における、日本の個人情報保護法に違反するリスクとして、特に問題になるのは、これも詳細は後述するが、プライバシーポリシーの表現における、法令に基づいた個人データの第三者開示の規定が適用されてしまう点である。この「法令」とは、米国カリフォルニア州や米国の法令を意味する。OpenAI 社は、米国カリフォルニア州法あるいは米国法に基づいて日本の利用企業の扱う個人データを、第三者に開示してしまう

ことが、契約上可能となってしまうことになる。このような契約を締結した上で、個人データを AI に入力した時点で、その個人データは、OpenAI 社によって第三者に開示されるリスクが生じるのであり、この場合、その時点で日本企業は個人情報保護法に違反していることになってしまう。

■ 第二. 『OpenAI Privacy policy November 4, 2024 版』について

『OpenAI Privacy policy November 4, 2024 版』

原文: <https://openai.com/policies/privacy-policy/>

※ OpenAI の AI サービスを、企業向けの API インターフェイスを呼び出す場合には、この『OpenAI Privacy policy』は適用されないと、同ポリシー前文部分に記載があります。ただし、企業ユーザーであっても、API を用いずに、OpenAI の ChatGPT の通常の画面・通常の契約で個人データを分析するケースも相当程度存在すると思われることから、『OpenAI Privacy policy』についても分析の対象としました。

1. Personal Data we collect

1. 当社が収集する個人データ

User Content: We collect Personal Data that you provide in the input to our Services ("Content"), including your prompts and other content you upload, such as files (opens in a new window), images (opens in a new window), and audio (opens in a new window), depending on the features you use.

ユーザーコンテンツ: 当社は、顧客がプロンプトやファイル、画像、音声等として入力したコンテンツの個人データを収集いたします。

⇒ OpenAI 社は、プロンプト入力される個人データを「収集」すると、プライバシーポリシーで明言している。よくある誤解として、設定画面でモデル学習に利用する機能を OFF に（オプトアウト）すれば（Enterprise 契約ではデフォルトで OFF である）収集・蓄積されないというものがある。だが、それは誤りではないか。本プライバシーポリシーをよく読むと、オプトアウトしても、単にモデル学習に利用されなくなるだけで、その他の目的ではおおいに利用されるし、また、米国カリフォルニア州法あるいは米国法が要求する場合は、第三者に開示されてしまうように読める。

2. How we use Personal Data

2. 当社による個人データの使用

We may use Personal Data for the following purposes:

当社は、以下の各目的で、個人データを使用することができるものとします:

- To improve and develop our Services and conduct research, for example to

develop new product features;

- 新しい製品機能を生み出すために、当社のサービスを改良・開発・研究する目的。
- To comply with legal obligations and to protect the rights, privacy, safety, or property of our users, OpenAI, or third parties.
- 法律上の義務を遵守するため、および（編注：契約当事者以外を含む）当社の顧客たち、当社自身および第三者の法的権利、プライバシー権利、安全および財産を保安するため。

⇒ まず、OpenAI 社は入力された個人データを「法律上の義務を遵守するため」に顧客の承諾無く勝手に「使用」することができると規定されている。そして、「法律上の義務」の「法律」とは、OpenAI 企業向け約款 15.12 節で規定されているとおり、米国カリフォルニア州法および米国のことである。

⇒ したがって、OpenAI 社と契約を締結する日本企業は、上記のとおり、個人データについて、OpenAI 社が米国カリフォルニア州法および米国の法を遵守する目的で、勝手に利用することについて承諾していることになる。

⇒ 次に、OpenAI 社は入力された個人データを「当社の顧客たち、当社自身および第三者の法的権利、プライバシー権利、安全および財産を保安するため」に顧客の承諾無く勝手に「使用」することができると規定されている。

⇒ したがって、OpenAI 社と契約を締結する日本企業は、上記のとおり、個人データについて、OpenAI 社が「当社の顧客たち、当社自身および第三者の法的権利、プライバシー権利、安全および財産を保安するため」という目的で、勝手に利用することについて承諾していることになる。

⇒ これらは、個人情報保護法上の問題を引き起こす。すなわち、第三者の利益のために個人データが使われることを承知していながら、OpenAI 社に個人データを入力する行為を構成するので、そのことが、個人情報保護法 27 条の第三者提供にあたり本人の同意がない場合は違法になるというものである。

⇒ だが、個人情報保護法 27 条 1 項 1 号除外事由に当てはまれば、違法とはならない。そこで、同条の「法令に基づく場合」の「法令」が、㊦ 日本国の法令のみを示すのか、それとも、㊧ 当該外国委託先企業の存する外国の法令も含むのかが、問題となる。これについて、日本政府は国会答弁で ㊦ であるとの公式見解を出している（2019 年 6 月 25 日衆議院答弁第 227 号）。この日本政府の公式見解に従う限り、同項 1 号除外事由が利用できない。

⇒ OpenAI の規定に基づけば、本人による同意取得が困難といえる特段の事情がない場合であっても、OpenAI 社は、「当社の顧客たち、当社自身および第三者の法的権利、プライバシー権利、安全および財産を保安するため」に、その本人の個人データを、第三者に提供できてしまうことになる。この場合、個人情報保護法 27 条 1 項 2 号除外事由の「本人の同意を得ることが困難であるとき」という、本人同意取得困難性の要件を充足しないから、違法になるのではないか。

We may also aggregate or de-identify Personal Data so that it no longer identifies you and use this information for the purposes described above, such as to analyze the way our Services are being used, to improve and add

features to them, and to conduct research. We will maintain and use de-identified information in de-identified form and not attempt to reidentify the information, unless required by law.

当社は、当社のサービスの利用状況を分析したり、当社のサービスを改良・新規開発・研究するといった、上述の目的の場合は、個人データを集約あるいは匿名化し、個人識別不能な状態に加工することができる（編注："may" であり、"shall" や "must" ではない）ものとします。この場合、当社はいったん匿名化されたデータをその状態で扱う予定であり、個人識別可能な状態に復元しない意思を有します（編注："will" であり、"shall" や "must" ではない）。ただし、法律によって要求された場合は、この限りではありません。

- ⇒ まず、この条項は、極めて注意して読まなければならない。OpenAI は入力される個人データを「集約」あるいは「匿名化」として述べるものであるが、それは OpenAI が改良行為を行なう場合に限られる。つまり、前述の、「(米国カリフォルニア州法および米国の) 法律上の義務を遵守するため、および当社の顧客たち、当社自身および第三者の法的権利、プライバシー権利、安全および財産を保安するため。」という目的の場合、データの「集約」あるいは「匿名化」は行なわれず、生のデータが使用されることになる。
- ⇒ 次に、(意図したか否かは不明であるが) この条項は非常に曖昧かつ脆弱な内容になっている。OpenAI が改良行為を行なう場合であっても、個人データを集約あるいは匿名化し、個人識別不能な状態に加工することが「できる（編注："may" であり、"shall" や "must" ではない）」と規定されているのである。そして、一度個人識別不能な状態にしたなら、「法律によって要求された場合」を除いては、個人識別可能な状態には復元しない意思がある（"will"）と記載されている。そもそも、英文契約書で通常利用される頻度が少なく曖昧な "will" をここで利用している点は、日本企業としては皆気にかかるであろう。だが、より重要な問題は、前記の「will」の義務は、未だ個人識別不能な状態にしていないデータに対しては適用されないという点である。日本企業は、OpenAI が改良行為を行なう場合は、前もって個人データは、必ず個人識別不能な状態に変形されると信じているが、この条項を読む限りでは、そうとは限らない。
- ⇒ 最後に、「法律によって要求された場合」は、一度個人識別不能な状態に加工したデータを、個人識別可能な状態に復元することができる、と規定されている。ここに大きな 2 つの問題がある。
 - ⇒ 1 つ目の、たいへん面白い問題は、「一度個人識別不能な状態に加工したデータ」であるはずなのに、「法律によって要求された場合」であればそれを「復元」できるのだ、という旨が記載されている点である。つまり、「一度個人識別不能な状態に加工」するとしていながら、「復元」が可能なのであれば、そもそも「一度個人識別不能な状態に加工」していないのではないか、という矛盾の存在がみられるのである。
 - ⇒ 2 つ目の問題は、前掲の問題と同じであり、「法律によって要求された場合」の「法律」とは、日本法ではなく、米国カリフォルニア州法および米国法を意味するという点である。

837 3. 個人情報の（編注：第三者への）開示

838

839 We may disclose your Personal Data in the following circumstances:

840 当社は、顧客の個人データを、以下の場合に（編注：第三者に）開示できるものと
841 します：

842

843 - Business Transfers: If we are involved in strategic transactions,
844 reorganization, bankruptcy, receivership, or transition of service to
845 another provider (collectively, a "Transaction"), your Personal Data may be
846 disclosed in the diligence process with counterparties and others assisting
847 with the Transaction and transferred to a successor or affiliate as part of
848 that Transaction along with other assets.

849 - 事業譲渡：当社が関わる戦略的取引、組織再編、破たん、管財あるいは事業譲渡
850（以下「取引等」といいます。）に関して、当社は、顧客の個人データを、取引を予
851 定している相手方による買収前評価手続きあるいはその支援者のために、譲渡され
852 る他の当社の財産と共に、開示することができるものとします。

853

854 ⇒ 問題点が2つある。(a) 包括承継となる合併や分割等ではなく、単なる事業の売
855 買である事業譲渡であっても、本条項は適用されてしまう。(b) OpenAI 社の事
856 業譲渡等の取引を予定している第三者が買収前評価手続きとして要求したならば、
857 OpenAI 社は、その第三者に対して、個人データを開示することができる。

858 ⇒ これらの事柄は、OpenAI 社の単独の意欲でいつでも発生させることができても
859 まう。すなわち、日本企業の入力した個人データは、いつでも OpenAI 社が指名
860 した、全く無関係の取引予定者（事業譲渡等が行なわれた場合ではなく、事業譲
861 渡前において）に対して開示されてしまうということである。OpenAI 社の利益
862 のために個人データが第三者に開示されるのである。日本企業が、上記のこのこ
863 とを同意した上で個人データを OpenAI 社のサービスに入力するとすれば、個人
864 情報保護法上の問題が発生する。

865

866 - Government Authorities or Other Third Parties: We may share your Personal
867 Data, including information about your interaction with our Services, with
868 government authorities, industry peers, or other third parties in
869 compliance with the law (i) if required to do so to comply with a legal
870 obligation, or in the good faith belief that such action is necessary to
871 comply with a legal obligation, (ii) to protect and defend our rights or
872 property, (iii) if we determine, in our sole discretion, that there is a
873 violation of our terms, policies, or the law; (iv) to detect or prevent
874 fraud or other illegal activity; (v) to protect the safety, security, and
875 integrity of our products, employees, users, or the public, or (vi) to
876 protect against legal liability.

877 - 政府機関およびその他の第三者：当社は顧客の個人データを、次の場合に、政府機
878 関、同業他社、あるいはその他の第三者に対して、適法に開示できるものとします：
879 (i) 法律上の義務を履行するよう請求されたか、あるいは、法律上の義務を履行す
880 るために必要であると誠実に信じる場合、(ii) 当社の法的権利あるいは財産を保護

する目的の場合、(iii) 当社による単独の裁量によって、当社の制定する規則、ポリシーあるいは法令に違反する行為があったと判断した場合、(iv) 詐欺あるいは違法行為を検出し抑制するため、(v) 安全、保安、あるいは当社の製品、従業員、他のユーザーや公衆の秩序を維持するために必要な場合、(vi) (当社が) 法的債務に對抗する場合。

⇒ まず、この条項の柱書では、OpenAI 社は個人データを「政府機関、同業他社、あるいはその他の第三者に対して、適法に開示できる」としている。「適法」の「法」とは、米国カリフォルニア州法および米国のことである (OpenAI 企業向け約款 15.12 節で規定)。開示先の「政府機関」とは、米国政府を含む。さらに、「同業他社、あるいはその他の第三者」に対しても開示できると記載されている。これはかなり重大な問題である。日本企業が、これらのことを認識せず、OpenAI 社を利用してしまうリスクがある。

⇒ 次に、(i) について、「法律上の義務」の「法律」とは、米国カリフォルニア州法および米国のことである (OpenAI 企業向け約款 15.12 節で規定)。これらの法律により請求された場合も、さらには、「法律上の義務を履行するために必要であると誠実に信じる場合」に自主的に行なう場合でも、OpenAI 社は、日本企業の個人データを第三者に勝手に開示してしまうことができる、という規定である。

⇒ 前述のとおり、日本政府は、個人情報保護法 27 条 1 項 1 号除外事由の「法令に基づく場合」の「法令」は、[ア](#) 日本国の法令のみを示す、と公式見解を示している (2019 年 6 月 25 日衆議院答弁第 227 号)。そのため、日本政府の立場と同じ立場で判断がなされた場合、OpenAI 社が米国カリフォルニア州法および米国の法律に基づいていつでも個人データを第三者開示してしまうということに同意した上で個人データを入力すれば、日本企業側が個人情報保護法違反となってしまう、という問題が生じる。

⇒ そして、(iii) は、さらに問題である。この条項によると、OpenAI 社は、なぜか、「当社による単独の裁量によって、当社の制定する規則、ポリシーあるいは法令に違反する行為があったと判断した」場合にも、第三者に対して、入力された個人データを開示できる、としているのである。(iv) 詐欺あるいは違法行為を検出し抑制するため、なども同様である。

⇒ すなわち、個人データを含むプロンプトのリクエスト内容から、OpenAI 社が上記のような場合に該当するとみなした場合は、利用日本企業の同意なく、勝手にその入力個人データが、無関係の第三者に提供されてしまうリスクがある。

4. Retention

4. 保持

We'll retain your Personal Data for only as long as we need in order to provide our Services to you, or for other legitimate business purposes such as resolving disputes, safety and security reasons, or complying with our legal obligations.

当社は、顧客の個人データを、顧客にサービスを提供するために必要な期間のほか、当社の適法なビジネス上の目的（法的紛争、安全や保安上の理由、他に法的に義務付

925 けられる規制に適合することを含む) で必要な限り保持し続けることができます。

926

927 ⇒ 本条項によると、日本企業が OpenAI のサービスに入力するプロンプト等の個人
928 データは、その日本企業の利益とは無関係に、OpenAI 社自身の利益のために保
929 持し続けることができる、と規定されている。つまり、日本企業が要求しても、
930 個人データを消すことはない、という意味である。

931 ⇒ 日本企業が、このことに同意した上で、個人データを OpenAI 社のサービスに入
932 力することは、OpenAI 社が個人データを扱うことになるのか否かに関わらず、
933 個人情報保護法上、違法になるのではないか。

934 ⇒ たとえ単なるデータの処理装置として OpenAI の AI サービスを利用してい
935 るという整理にするにしても、上記の条項によると、その入力データは、入
936 力された途端、日本企業の管理支配を離れて OpenAI 社が上記目的で、同社
937 の利益のために必要な限り、保持し続けることができてしまうことになる。
938 その保持されたデータは、同社あるいは第三者の利益のための第 2 節あるい
939 は第 3 節で定められた利益のために、同社によって使用、あるいは、同社か
940 ら第三者開示されることになる。

941 ⇒ 上記のような OpenAI 社の意図を知った上で、日本企業が OpenAI 社のサー
942 ビスに個人データを入力することは、まさにその日本企業の視点からみた場
943 合は、委託の範囲を逸脱した第三者提供 (27 条 1 項) (なお、OpenAI 社の
944 視点からみた場合は、18 条 1 項の目的外利用) にあたるので、本人の同意
945 がなければ違法となるのではないか。

946

947 As noted above, we may use Content you provide us to improve our Services,
948 for example to train the models that power ChatGPT. Read our instructions on
949 how you can opt out of our use of your Content to train our models.

950 上述のとおり、当社は顧客が提供した個人データを当社のサービスの向上、たとえば
951 ChatGPT のモデルの学習のために利用することができるものとします。顧客はデータ
952 を ChatGPT モデルで学習しないように設定できます。説明書をお読みください。

953

954 ⇒ ここで、いきなりオプトアウトの話が出てくる。だが、前述したとおり、これで
955 禁止することができるのは、ChatGPT モデルの改良行為にその個人データが利用
956 されないようにするという点のみである。それ以外の OpenAI 社による利用・開
957 示・保持行為は、一切禁止されない。日本企業は、これらが行なわれることをプ
958 ライバシーポリシー上予め承諾させられることになる。

959

960 9. Changes to the privacy policy

961 9. プライバシーポリシーの変更

962

963 We may update this Privacy Policy from time to time. When we do, we will
964 publish an updated version and effective date on this page, unless another
965 type of notice is required by applicable law.

966 当社は、随時プライバシーポリシーを更新することができるものとします。プライバ
967 シーポリシーの更新は、別途適用される法律で要求されない限り、更新後のバージョ
968 ンと適用日を、この Web サイトに掲載することによります。

- ⇒ プライバシーポリシーは、OpenAI 社側の個人データの保護水準の義務の設定のために重要な役割を担うところ、この規約によれば、「別途適用される法律で要求されない限り」いつでも変更されることになる。顧客はその内容に同意したとみなされる。日本民法における定型約款の変更の規則は、準拠法が米国カリフォルニア州法および米国法であることから、適用されない。
- ⇒ ここで発生する個人情報保護法上の問題は、OpenAI 企業向け約款第 14.1 節で述べた問題と同様である。

■ 第三. 『Data Processing Addendum (データ処理委託特約) February 15, 2024 版』について

『Data Processing Addendum (データ処理委託特約) February 15, 2024 版』

原文: <https://openai.com/policies/data-processing-addendum/>』

This Data Processing Addendum ("DPA") governs OpenAI's processing of Customer Data (i) provided by Customer to OpenAI through OpenAI's API or any OpenAI services for businesses ("API Services") or (ii) pursuant to OpenAI's provision of the ChatGPT Enterprise service for businesses (the "ChatGPT Enterprise Services") (for purposes of this DPA, the API Services and ChatGPT Enterprise Services are together the "Services") under the terms of the OpenAI Business Terms (located at openai.com/policies/business-terms), Enterprise Agreement, or other agreement between Customer and OpenAI governing Customer's use of the Services (the "Agreement") and is hereby incorporated into the Agreement. If and to the extent language in this DPA conflicts with the Agreement, the conflicting terms in this DPA shall control. Capitalized terms not defined in this DPA have the meaning set forth in the Agreement. For the purposes of this DPA only, "Customer" includes any affiliate entity of Customer's that (a) has entered into an Order Form with OpenAI and that (b) directly or indirectly, through one or more intermediaries controls, is controlled by, or is under common control with Customer.

このデータ処理委託特約（「DPA」）は、OpenAI 企業向け約款、Enterprise Agreement、あるいは顧客と OpenAI との間でのその他の契約（以下「本契約」）における、(i) OpenAI の API あるいはその他のビジネス向け OpenAI サービス（「API サービス」）を通じて顧客から提供された、あるいは (ii) ChatGPT Enterprise Services (API サービス等と併せて「本サービス」）に基づいて供給された、OpenAI 社による顧客データの処理を規定するものであり、本契約の内容を構成するものです。DPA の内容と元の契約とが矛盾する場合は、DPA の規定に従うものとします。（以下略）

OpenAI and Customer each agree to comply with their respective obligations under applicable data privacy and data protection laws (collectively, "Data

Protection Laws") in connection with the Services. Data Protection Laws may include, depending on the circumstances, Cal. Civ. Code § § 1798.100 et seq., as amended by the California Privacy Rights Act of 2020 (the California Consumer Privacy Act) ("CCPA"), Colo. Rev. Stat. § § 6-1-1301 et seq. (the Colorado Privacy Act) ("CPA"), Connecticut's Data Privacy Act ("CTDPA"), Utah Code Ann. § § 13-61-101 et seq. (the Utah Consumer Privacy Act) ("UCPA"), VA Code Ann. § § 59.1-575 et seq. (the Virginia Consumer Data Protection Act) ("VCDPA") (collectively "U.S. Privacy Laws"), and the United Kingdom and/or European Union General Data Protection Regulation (Regulation (EU) 2016/679) (collectively the "GDPR"), and applicable subordinate legislation and regulations implementing those laws.

OpenAI 社と顧客は、本サービスに関連して適用されるデータプライバシーおよびデータ保護法（これらを総称して「データ保護法」といいます。）に基づく各自の義務を遵守することに同意するものとします。「データ保護法」とは、状況に応じて、カリフォルニア州プライバシー権法（「CCPA」、詳細略）、コロラド州プライバシー法（「CPA」、詳細略）、コネティカット州データプライバシー法（「CTDPA」、詳細略）、ユタ州消費者プライバシー法（「UCPA」、詳細略）、ヴァージニア州消費者データプライバシー法（「VCDPA」、詳細略）（これらを総称して、「米国プライバシー法」といいます）、および英国および / または EU の一般データ保護規約（総称して「GDPR」、詳細略）、およびこれらの法律に関して適用される下位法ならびにこれらの法律の施行規則を含むものとします。

In connection with the Agreement, Customer is the person that determines the purposes and means for which Customer Data (as defined below) is processed (a "Data Controller"), whereas OpenAI processes Customer Data in accordance with the Data Controller's instructions and on behalf of the Data Controller (as a "Data Processor"). "Data Controller" and "Data Processor" also mean the equivalent concepts under Data Protection Laws. For the purposes of the Agreement and this DPA, (i) "Personal Data" has the meaning assigned to the term "personal data" or "personal information" under applicable Data Protection Laws; and (ii) "Customer Data" means Personal Data that Customer provides to OpenAI that OpenAI processes on behalf of Customer to provide the Services. OpenAI will process Customer Data as Customer's Data Processor to provide or maintain the Services and for the purposes set forth in this DPA, the Agreement and/or in any other applicable agreements between Customer and OpenAI.

本契約において、顧客は、「顧客データ」の処理に関する目的および手段を決定する者（以下「データ管理者」）であり、OpenAI 社は、データ管理者の指示に従い、データ管理者に代わって顧客データを処理します（以下「データ処理者」）。「データ管理者」および「データ処理者」という用語は、データ保護法における同等の概念も意味します。本契約および本データ処理契約（DPA）の目的のために、(i) 「個人データ」とは、適用されるデータ保護法において「個人データ」または「個人情報」という用語に割り当てられた意味を有し、(ii) 「顧客データ」とは、顧客が OpenAI に提供し、OpenAI 社が顧客に代わってサービスを提供するために処理する個人データを指します。

1057 OpenAI 社は、サービスを提供または維持するためおよび本 DPA、本契約および顧客と
1058 OpenAI 社との間のその他の適用可能な契約に定められた目的のために、顧客のデータ
1059 処理者として顧客データを処理します。

1060
1061 ⇒ データ処理委託特約 (DPA) では、OpenAI 社が主体となって「顧客データ」を
1062 「処理」として明記されている。ところで、よく AI 処理を行なうことが個人
1063 データの取扱いの「委託」 (= 広義の第三者提供) にあたるとかが問題と
1064 なり、個人情報保護委員会の、いわゆる「クラウド例外」にあたると「委託」
1065 にあたらないとして処理してしまうケースもあると聞く (仮に「委託」にあた
1066 らないのであれば、個人本人からの同意を得なくとも、AI 会社が米国企業である
1067 場合において、法 28 条 1 項の相当措置の担保義務が不要になるためである)。
1068 個人情報保護委員会の、いわゆるクラウド例外においては、「…クラウドサー
1069 ビス提供事業者が、当該個人データを取り扱わないこととなっている場合」には、
1070 本人の同意が必要な第三者提供や委託に該当しないものとされている。しかしな
1071 がら、OpenAI の上記約款に基づけば、明確に、OpenAI 社がデータ処理の主体と
1072 して規定されているので、いわゆるクラウド例外は利用できないことになってし
1073 まう。すると、原則として、法 28 条 1 項の「あらかじめ外国にある第三者へ
1074 の提供を認める旨の本人の同意を得なければならない」が適用されることになっ
1075 てしまう。これを免れるためには、日本ユーザー企業は、OpenAI 社に対して相
1076 当措置を講じさせる義務を負うことになる。各日本ユーザー企業は、それぞれ、
1077 実際に OpenAI 社のシステムに対して、適切に監理しなければならない。しかし、
1078 これまでに述べたとおり、OpenAI 社のシステムを適切に監理するのは、實際上、
1079 ユーザー企業側に、かなりの手数と技術力が必要とされてしまうので、現実的で
1080 はない場合も多い。そこで、結局は、OpenAI 社という「外国にある第三者」へ
1081 の提供を認める旨の本人の同意を得なければならないことになってしまう。
1082 ⇒ ユーザー企業 (「A」とする) と OpenAI 社 (「B」とする) との間に、日本国内
1083 の第三者 (「C」とする) を個人情報の取扱いの受託者として介在させ、A が C
1084 を API 呼び出しし、C が B を API 呼び出しするような方法を使えば、C は A
1085 からみて日本国内の受託業者であるので、本人同意を得ることなく、この問題が
1086 解決できるのではないかと、われわれは、安易に考えてしまうかも知れない。し
1087 かし、この手法では、この問題は解決できない。なぜならば、A においては、C
1088 が国内企業であっても、C に対する安全管理措置義務 (法 23 条)、委託先の監
1089 督義務 (法 25 条) を免れることができないので、結局 A は C に対して、C か
1090 らの再委託先である B に対する法 28 条 1 項にかかる相当措置が担保されてい
1091 ることを要求せざるを得ないためである。そのような担保があることを C が A
1092 に対して契約上および技術上保証してくれない限り、A は C に対して委託して
1093 はならず、これに A が違反すると、A が個人情報保護法違反 (法 23 条、法 25
1094 条) となってしまうためである。そもそも、そういう抜け穴を防ぐために、日本
1095 の個人情報保護法は、緻密に組み立てられているのである。結局、A → C → B
1096 の抜け穴を通ることはできず、結局は、OpenAI 社という「外国にある第三者」
1097 への提供を認める旨の本人の同意を得なければならないことになってしまう。

1098
1099 2. Notice to Customer

1100 2. 顧客への通知

1101
1102 OpenAI will inform Customer if OpenAI becomes aware of:
1103 a. any legally binding request for disclosure of Customer Data by a law
1104 enforcement authority, unless OpenAI is otherwise forbidden by law to inform
1105 Customer, for example to preserve the confidentiality of an investigation by
1106 law enforcement authorities; b. any notice, inquiry or investigation by an
1107 independent public authority established by a member state pursuant to
1108 Article 51 of the GDPR (a "Supervisory Authority") with respect to Customer
1109 Data;

1110 OpenAI は、次のことが発生した場合に顧客に通知をいたします: a. 法執行機関によ
1111 る顧客データの開示に対する法的拘束力のある要求があった場合。ただし、法執行機
1112 関による調査の機密性を保持するために、OpenAI が顧客に通知することを法律で禁じ
1113 られている場合はこの限りではありません。b. GDPR 第 51 条に従って加盟国が設立
1114 した独立公的機関（以下「監督機関」）による顧客データに関する通知、照会、調査。

1115

1116 ⇒ この条項により、OpenAI 社は、① 法執行機関による顧客データの開示に対する
1117 法的拘束力のある要求があった場合、② GDPR 第 51 条に従って加盟国が設立し
1118 た独立公的機関による顧客データに関する通知、照会、調査があった場合に、顧
1119 客に通知すると規定されている。特に問題となるのが ① である。① では、
1120 「ただし、法執行機関による調査の機密性を保持するために、OpenAI が顧客に
1121 通知することを法律で禁じられている場合はこの限りではありません。」とも規
1122 定されている。すなわち、OpenAI 社は、「法執行機関」から、個人データを提
1123 出せよという「法的拘束力のある要求」があり、かつ、通知が禁止されている場
1124 合には、顧客に対して事前通知することなく、その個人データを、「法執行機
1125 関」に提供してよいという規定になってしまっている。

1126 ⇒ ここで、「法執行機関」には、少なくとも OpenAI 社の所在する米国連邦政府あ
1127 るいは米国カリフォルニア州政府の法執行機関が含まれるはずである。なぜなら
1128 ば、OpenAI 社の役員・従業員たちは、物理的強制力によって、これらの米国の
1129 法執行機関からの強制を受ける立場にあるためである。

1130 ⇒ すると、次のような危険が発生する。日本のユーザー企業が個人データを含むプ
1131 ロンプトを OpenAI で AI 処理実行していたところ、捜査のために（その捜査は、
1132 日本の個人情報保護法 27 条 1 項 2 号のような「人の生命、身体又は財産の保
1133 護のために必要がある場合」に該当するような緊急性のない、通常の捜査とす
1134 る）、そのデータを米国の「法執行機関」が提出せよと OpenAI 社に要求し、か
1135 かつ、通知禁止命令が付加されていたとする。この可能性は、いつでも発生し得る。
1136 そして、「法執行機関」は、日本のユーザー企業と OpenAI 社との間のデータ委
1137 託処理契約においては第三者にあたる。つまり、上記規約が存在している限り、
1138 日本企業が OpenAI 社に対して送付した個人データを含むプロンプトの内容が、
1139 いつでも、その個人の同意なく、まったく無関係の米国の「法執行機関」という
1140 第三者に提供されてしまうことを意味する。

1141 ⇒ 前述のとおり、日本政府は、個人情報保護法 27 条 1 項 1 号除外事由の「法
1142 令に基づく場合」の「法令」は、日本国の法令のみを示す、と公式見解を示し
1143 ている（2019 年 6 月 25 日衆議院答弁第 227 号）。したがって、OpenAI 社
1144 が、米国の「法執行機関」の米国の法律に基づく要求によって個人データを提

供することは、仮に OpenAI 社が日本の個人情報保護法を遵守する意図があるとしても、日本政府の前記見解に従う限り、日本の個人情報保護法 27 条 1 項 1 号に該当せず、本人の同意がない限り、日本の個人情報保護法に違反することになってしまう。だが、この想定ケースでは、通知禁止命令が付加されているので、本人の同意を得ることは不可能なはずである。

⇒ また、上記規定が存在する限り、日本のユーザー企業は、仮に OpenAI 社が日本の個人情報保護法 28 条 1 項における「個人データの取扱いについてこの節の規定により個人情報取扱事業者が講ずべきこととされている措置に相当する措置（「相当措置」）を継続的に講ずるために必要なものとして個人情報保護委員会規則で定める基準に適合する体制を整備している者」という例外を利用することができなくなってしまう。個人情報保護委員会「個人情報の保護に関する法律についてのガイドライン（外国にある第三者への提供編）」の「4-2-11 第三者提供の制限（法第 27 条の趣旨に沿った措置）」には、「外国にある第三者等は、個人データの第三者への提供に当たり、あらかじめ本人の同意を得ないで提供してはならない。」との記載がある。したがって、日本ユーザー企業は、OpenAI 社から、「米国の捜査機関（第三者）から、たとえ当社が処理を委託している個人データを開示せよという命令があっても、当該第三者に提供をしてはならない。」という事前の合意を得なければならないはずである。しかし、本条項が存在することは、このような事前の合意が不可能であることを意味する [※ 5]。

⇒ ※ 5: OpenAI 社のこの DPA を締結する Web フォームには、
「Unfortunately, we are unable to review or sign DPAs provided by our customers or customize our DPA on a case by case basis.」
とあり、DPA の内容について、この雛形の DPA 以外の個別交渉には応じることが「不可能である」旨の記載がある。

⇒ したがって、原則通り、日本の個人情報保護法 28 条 1 項に基づき、OpenAI 社を利用して個人データを分析する場合は、あらかじめ各個人の同意を得て回る必要があるということになるのではないかと。・・・ ③

⇒ あるいは、OpenAI 社が、米国の捜査機関（第三者）から、たとえ受託個人データを開示せよという命令があっても、当該第三者に提供をすることはないというように、条項を是正してくれない限り、日本ユーザー企業の解決方法として、あらかじめ、日本において、OpenAI を用いて個人データを分析処理しようとしているすべての個人に対して、事前に、「あなたの個人データを、OpenAI 社を通じて、"米国合衆国政府あるいは州政府の捜査機関等" が要求したときにいつでも提供することについての同意」を得ておく必要があるように思われる。しかし、この方法でも、結局は OpenAI 社を利用して個人データを分析することについて、あらかじめ各個人の同意を得て回る必要があるということになるので、③ と比較して、大差ないように思える。

8. Term; Data Return and Deletion

8. 期間; データの返却および削除

This DPA shall remain in effect as long as OpenAI carries out Customer Data processing operations on Customer's behalf or until the termination of the

1189 Agreement (and all Customer Data has been returned or deleted in accordance
1190 with this DPA). OpenAI will retain API Service Customer Data sent through the
1191 API for a maximum of thirty (30) days, after which it will be deleted, except
1192 where OpenAI is required to retain copies under applicable laws, in which
1193 case OpenAI will isolate and protect that Customer Data from any further
1194 processing except to the extent required by applicable laws. OpenAI will
1195 retain ChatGPT Enterprise Service Customer Data during the term of the
1196 Agreement, unless otherwise stated in the Agreement or Order Form. On the
1197 termination of the DPA, OpenAI will direct each Subprocessor to delete the
1198 Customer Data within thirty (30) days of the DPA's termination, unless
1199 prohibited by law. For clarity, OpenAI may continue to process information
1200 derived from Customer Data that has been deidentified, anonymized, and/or
1201 aggregated such that the data is no longer considered Personal Data under
1202 applicable Data Protection Laws and in a manner that does not identify
1203 individuals or Customer to improve OpenAI's systems and services.

1204 本データ処理契約（DPA）は、OpenAI 社が顧客に代わって顧客データの処理業務を実
1205 施している限り、または契約が終了するまで有効とします（すべての顧客データが本
1206 DPA に従って返却または削除されるまで）。OpenAI 社は、API を通じて送信された
1207 API サービスの顧客データを最大 30 日間保持し、その後削除します。ただし、適用
1208 法により OpenAI 社がコピーを保持することが要求される場合、OpenAI 社はその顧客
1209 データを隔離し、適用法で要求される範囲を除き、それ以上の処理から保護します。
1210 OpenAI 社は、契約期間中、ChatGPT エンタープライズサービスの顧客データを保持し
1211 ますが、契約または注文書で別途記載がない限りこの限りではありません。DPA 終了
1212 時に、OpenAI 社は各サブプロセッサに対し、法により禁止されていない限り、DPA
1213 終了後 30 日以内に顧客データを削除するよう指示します。明確にするために、
1214 OpenAI 社は、適用されるデータ保護法に基づき個人データと見なされなくなった、識
1215 別解除、匿名化、および / または集約された顧客データから得られた情報を、個人ま
1216 たは顧客を識別しない方法で OpenAI のシステムおよびサービスを改善するために処
1217 理し続けることができます。

1218
1219 ⇒ 「適用法」とは、前述のとおり、米国カリフォルニア州法および米国法である。
1220 そのため、前述と同様のケースで、米国の捜査機関（第三者）から、データの
1221 保持を要求された場合は、彼ら第三者のために、そのデータが長期間保持され、
1222 削除されない危険性がある。

1223
1224

1225 ■ 第四. 『OpenAI における企業プライバシー 2024 年 10 月 31 日版』について

1226

1227 『OpenAI における企業プライバシー 2024 年 10 月 31 日版』

1228 原文: <https://openai.com/ja-JP/enterprise-privacy/>

1229

1230 「サービス全般」

1231 Q. OpenAI は顧客のビジネスデータの検証を行いますか？

1232 A. OpenAI のサービスに提供されたビジネスデータに対して、当社サービスの利用法

に対する理解を深めることなどを目的として、自動コンテンツ分類ツールや安全性ツールが使用される場合があります。作成される分類は、ビジネスデータに関するメタデータですが、そこにビジネスデータそのものが含まれることはありません。ビジネスデータの検証は人間によってのみ行われます。詳細は下記のサービスごとの説明をご参照ください。

- ⇒ 「ビジネスデータ」とは、ChatGPT や OpenAI API の入出力プロンプトデータを含む（同 FAQ 参照）。そして、この FAQ 項目では、「④当社サービスの利用法に対する理解を深めることなど」を目的として、入力データをもとに分類データを生成する、だが、この分類データはビジネスデータに対するメタデータであり、ビジネスデータそのものは、②「ビジネスデータの検証は人間によってのみ行われ」る、と規定されている。
- ⇒ すなわち、この FAQ 項目は、OpenAI 社が次のことを行なうことができることを意味しているのである。(a) まず、「自動コンテンツ分類ツールや安全性ツール」などの AI 的なソフトウェアによって、顧客のすべての入出力データを自動分類する。(b) その分類結果を保持する。(c) 「当社サービスの利用法に対する理解を深めることなど」を目的として、OpenAI 社の「人間」が、分類結果から参照される元の顧客の入出力データを「検証」する。
- ⇒ ここで、「ビジネスデータ」は、顧客の入力したプロンプトそのものであるから、もちろん、生の個人データ（匿名化等の処理がされていないもの）が含まれる。
- ⇒ この FAQ 項目の「当社サービスの利用法に対する理解を深めることなどを目的として」という「目的」の表記は、顧客のための契約上の債務履行に必要なトラブルシューティング目的ではなく、単なる OpenAI 社の利益のためのサービス改良行為に過ぎない。この FAQ 項目は、明確に、OpenAI 社の利益のための目的として個人データを OpenAI 社の「人間」が目視し検証分析することを、認めているのである。
- ⇒ そうすると、次のことがいえる。OpenAI 社は、顧客のためではなく、OpenAI 社自身の利益のために、「当社サービスの利用法に対する理解を深めることなど」を目的として、いつでも、日本企業がプロンプト入力した生の個人データの本文を、OpenAI 社の従業員（「人間」と記載されている）によって、目視し、分析することができる、ということである。これでは、利用する日本企業側が、個人情報保護法に明確に違反することになってしまう。すなわち、「生成 AI サービスの利用に関する注意喚起等 令和 5 年 6 月 2 日 個人情報保護委員会」の「(1) ②」の「当該個人データが当該プロンプトに対する応答結果の出力以外の目的で取り扱われる場合」に該当してしまうことになることが懸念される (OpenAI 社による「当社サービスの利用法に対する理解を深めることなど」を目的とした個人データの利用は、明らかに、「当該プロンプトに対する応答結果の出力以外の目的」である)。

「生成 AI サービスの利用に関する注意喚起等 令和 5 年 6 月 2 日 個人情報保護委員会」

https://www.ppc.go.jp/files/pdf/230602_alert_generative_AI_service.pdf

- ※ 1: OpenAI の企業向けサービスには、API でデータを AI インプットするものがある。OpenAI の API を用いて、ユーザー企業が個人情報をインプットする行為は、個人データ処理の「委託」にあたるとされる。前述の「第三、『Data Processing Addendum (データ処理委託特約) February 15, 2024 版』について」も参照。
- 【参考文献】 柿沼太一他「パネルディスカッション: ChatGPT と生成 AI に関する法的倫理的課題」 NBL 1245 号 (2023 年 7 月 1 日発行) 40 頁) での田中浩之弁護士の説明:
- 「割とはっきりしているのが、OpenAI の場合、API を使った場合は DPA (data processing addendum、データ処理契約) を結ぶことができ、この DPA は GDPR も意識したグローバルな定めになっており、機械学習にも使われないことが約束された形で、OpenAI の委託先としての役割が定められているので、API を使えば、委託としての整理ができることになります。」
- ※ 2: OpenAI 社は、外部投資家による多額の投資を受け、おそらく短期間の開発が求められた結果、極めて大規模かつ複雑な同社 AI サービス基盤を短期間で構築する際に、自社の技術能力だけでは不足、少なくとも 11 個もの外部クラウドベンダの多数のサービスを組み合わせて、急いでシステムを構築した。そして、それら外部サービスに、セキュリティを維持するための重要な部分が依存してしまっている。これら依存先の多数の外部クラウドシステムは、それぞれ、異なる社外の主体が、ばらばらにプログラミングして、構築・運用しているものである。セキュリティの観点でみると、われわれは、これらの多数の外部クラウドサービス基盤の 1 箇所にもセキュリティ侵害を許せば、処理あるいは保管される個人データが大規模に漏えいする危険がある。多数の環で直列的に接続された鎖の脆弱さは、最も弱い環の部分から生じるためである。
- <https://openai.com/policies/sub-processor-list/> のリストのように、OpenAI 社のセキュリティは、現在、たとえば、次のような外部クラウドシステムのサービスに依存している。
- (ア) 顧客は、OpenAI の API エンドポイントに対して、機密の個人データや API を呼び出すための認証鍵を入力する。ここでは、顧客との間で SSL で暗号化がなされているが、実はこの SSL 暗号化の部分の SSL ロードバランサエンジンは OpenAI 社が自ら構築・運用せず、他社である Cloudflare 社の基盤を利用している。AI 入出力データのセキュリティは、Cloudflare 社の SSL 基盤の不可侵性に依存していることになる。
- (i) より具体的に述べると、これは、次のことを意味する。日本のユーザー企業が OpenAI 社に対して <https://chatgpt.com/> (ChatGPT の Web 画面) あるいは <https://api.openai.com/> (OpenAI の API エンドポイント [1]) を経由して個人データ等の機密情報をプロンプトで入力し、AI 処理の結果 (これも機密情報である) を受け取るが、この際、ユーザー企業は、自身のクライアントと OpenAI 社のサーバーとの間で HTTPS 通信 (SSL による安全な通信) が直接確立されており、この二者以外の

者がその内容を読み取ることは技術的に不可能であると信じている場合が多い。しかしながら、実際には、chatgpt.com と api.openai.com の HTTPS サーバーは Cloudflare 社の公衆向けロードバランサ基盤で動作しており、Cloudflare 社が chatgpt.com と api.openai.com の SSL 証明書の秘密鍵を保管している。HTTPS 通信を終端する（暗号化されたデータを解読して、平文を取り出す）のは、実は、OpenAI 社ではなく Cloudflare 社のサーバーである。そして、そのサーバーは OpenAI 社が管理しているのではなく Cloudflare 社が管理している。

[1] <https://platform.openai.com/docs/api-reference/introduction>

(ii) このことは、chatgpt.com と api.openai.com の HTTPS サーバーに OpenSSL 等の SSL クライアントを用いて直接接続してみて、GET / POST 等のリクエストを送付し、その応答結果を注意深く観察すれば判明する。HTTP 応答のヘッダ内容には、「Server: cloudflare」というヘッダ文字が付加されていることが分かる。このヘッダ文字が挿入されている事実から、HTTPS 通信が一度 Cloudflare 社によって解読されていること、顧客と OpenAI 社との間の通信は完全に暗号化されておらず途中にこれを平文で読み出している第三者が介在することを意味する。

(iii) したがって、Cloudflare 社のサーバー管理を行なう高度な特権を有する従業員は、自らその意思が生じた場合、あるいは第三者に強制された場合、OpenAI 社のコントロール範囲外において、顧客と OpenAI 社との間を流れる入力プロンプト、出力プロンプトのいずれも、平文で読み取ることができる。あるいは、万一、Cloudflare 社の、OpenAI 社を含めてそれ以外の大量のユーザーの SSL 通信を処理している大規模 SSL 処理基盤のプログラムに脆弱性が存在するか、あるいはその他の攻撃手法により、サイバー攻撃者による Cloudflare 社の特権部分への侵入を許せば、同サイバー攻撃者は日本ユーザー企業が OpenAI 社を信用して入出力しているすべての機密 AI プロンプトおよび AI 処理結果を奪取することができてしまう。

(iv) また、ユーザーと OpenAI 社との間の認証については、chatgpt.com においては Cookie ヘッダに基づいたセッションキーベースの認証を、api.openai.com においては「Authorization:」ヘッダに記載する API キー文字列ベースの認証を利用することになる。ところが、これらの文字列は、(iii) の入出力プロンプトと同様に、Cloudflare 社のコンピュータで一度 SSL 暗号化が復号化され、同社のコンピュータはこれを平文として処理している。Cloudflare 社のシステムに対するセキュリティ侵害があった場合は、上記のように、ログイン済みのセッションが乗っ取られ、あるいは、API キーも奪取されてしまう。

(v) これは、「自身の入出力プロンプトの内容は、インターネットを通過する際、SSL によって OpenAI 社との間で直接暗号化され保護されている

1365 はずで、OpenAI 社以外の第三者によって読み取られることはあり得ない
1366 い」と信じている日本のユーザー企業にとって、意外な盲点である。実
1367 際には、第三者である Cloudflare 社が毎回平文に解読して、
1368 Cloudflare 社の管理するコンピュータ上にロードされ、平文の状態で
1369 Cloudflare 社の作ったソフトウェアと同社の所有する CPU によって読
1370 み取られている（「Server: cloudflare」というヘッダ文字が付加され
1371 ていることから明らかである）。

1372
1373 さて、OpenAI 社は、個人情報保護法上、プライバシー保護レベルが日
1374 本と同等以上の水準にないとされている米国 [2] の企業であるため、
1375 日本企業が、個人データの分析に OpenAI を利用する場合は、① 事前
1376 にすべての個人から同意を得るか、あるいは、② 個人情報保護法 28
1377 条 1 項の例外の要件である相当措置整備の担保を OpenAI 社に対して
1378 確保する必要がある。

1379
1380 [2] 「個人の権利利益を保護する上で我が国と同等の水準にあると認め
1381 られる個人情報の保護に関する制度を有している外国等」（平成 31
1382 年個人情報保護委員会告示第 1 号）

1383 https://www.ppc.go.jp/files/pdf/190123_h31iinkaikokuji01.pdf

1384
1385 ここで、日本企業は、多くのケースでは ② を望むと思われるが、②
1386 の場合は、OpenAI 社のシステムだけでなく、OpenAI 社との間で入出力
1387 されるプロンプトを平文で処理している Cloudflare 社のシステムに対
1388 しても相当措置整備の担保を確保する必要があるということになりそう
1389 である。委託先の監理としては、OpenAI 社の自前のシステムの安全性
1390 のみを監理するだけでは不十分であり、OpenAI 社からの SSL 処理部分
1391 の再委託先である Cloudflare 社のシステムの安全性も追加で監理しな
1392 ければならないということである（個人情報保護法 23 条、25 条、28
1393 条 1 項、個人情報保護法施行規則 16 条 1 号、個人情報の保護に関する
1394 法律についてのガイドライン（外国にある第三者への提供編）4-2）。

1395
1396 なぜならば、前述のとおり、Cloudflare 社のシステムが侵害された場
1397 合、すべての個人データはそこから漏えいしてしまうことになるため
1398 ある。Cloudflare 社のシステムの体制は、OpenAI 社のコントロール範
1399 囲外であるため、日本のユーザー企業は、OpenAI 社のシステムだけを
1400 監理すれば足りるということにならずに、Cloudflare 社のシステム体制
1401 に係る安全性についても継続的に監理しなければならない（単に
1402 OpenAI 社が Cloudflare 社に対して何らかの安全性を契約上担保させ
1403 ているとしても（その場合でも、OpenAI 社と Cloudflare 社との間の
1404 契約内容およびその担保が十分であるかどうかのようにして契約書をチェッ
1405 クすればよいのかという問題がある）、それだけでは、日本のユーザー
1406 企業が自らの個人情報保護法上の義務を免れることにはならないので、
1407 結構大変である）。

1408 → 個人情報保護委員会 「個人情報の保護に関する法律についての

ガイドライン（外国にある第三者への提供編）」4-1 参照。「個人データの提供先である外国にある第三者が、我が国の個人情報取扱事業者が講ずべきこととされている措置に相当する措置を継続的に講ずることを『担保することができる』方法である必要がある」と規定されている。

これをどのように実現するのか。これこそが、OpenAI を用いて個人情報の分析を行ないたいと考える、日本の "各" ユーザー企業が、それぞれ個別に解決しなければならない課題である。日本の各ユーザー企業が、実際に、これらのシステム全部の安全性を監理することができるのであれば、問題はない。だが、現実的に、直接の契約関係がない Cloudflare 社に対して必要な監査を行ない、システム内部の安全性を確認させてもらうことは、実際困難であるか、あるいは、相当な手数と技術力と交渉力が要求されるのではないと思われる。

- (イ) 顧客は、OpenAI の Web 管理者コンソール画面に対して、管理者権限でログインしたのちに、その顧客としてなしえるほぼすべての操作が可能である。したがって、ユーザー認証が極めて重要である。ここでも、OpenAI は自ら認証処理を実施せず、他社である Okta 社の Auth0 という SaaS 型の認証サービスを呼び出して認証してもらっている。認証セキュリティは、Okta 社の Auth0 の不可侵性に依存していることになる。

すると、(ア)と同様に、日本ユーザー企業としては、処理対象の個人データの各個人の事前の同意を得ていない場合、自らの責任で、Okta 社の Auth0 システムについても、相当措置整備の担保を確保する必要がある（個人情報保護法 28 条 1 項の例外の要件）ことになる。これは不可能ではないが、(ア)の Cloudflare 社のシステムに対する監理と同様相当な手数と技術力と交渉力が要求される。

- (ウ) OpenAI は、他社である Microsoft 社の Azure クラウド基盤上で構築されている。OpenAI 社の最高レベルの特権を有するシステム開発・運用担当の従業員は、Azure クラウド基盤上で動作している仮想マシンに対する管理者権限 (root 権限) を有する。しかし、Azure クラウド基盤そのものの管理者権限は他社である Microsoft 社の従業員が有しており、OpenAI 社のコントロール範囲外である。また、OpenAI 社による Azure クラウド基盤への特権アクセスは Microsoft の自作プログラムである認証システムによって制御されている。AI サービス基盤のセキュリティは、これらの要素の不可侵性に依存していることになる。

すると、(ア)と同様に、日本ユーザー企業としては、処理対象の個人データの各個人の事前の同意を得ていない場合、自らの責任で、Microsoft の自作クラウド基盤やそのクラウド基盤の自作認証システムについても、相当措置整備の担保を確保する必要がある（個人情報保護法 28 条 1 項の例外の要件）ことになる。これも不可能ではないが、(ア)の Cloudflare 社のシステ

ムに対する監理と同様、相当な手数と技術力と交渉力が要求される。

(エ) その他、OpenAI は、少なくとも、8 個の外部クラウドサービスに依存している。詳しくは、前述 URL を参照。

これらの OpenAI の依存先の外部クラウドサービス 1 つずつが直ちに危険であるというわけではない。これらの外部クラウドサービスには、必ず、未知の脆弱性が存在するが（かつ、クラウドサービスを動かすプログラム群はバイナリすら公開されておらず、脆弱性を発見し減らすために必須である多数の第三者による環視による継続的検査を経ていない。すなわち、バイナリが公開されているような伝統的ソフトウェア、たとえば Windows や Office のプログラムと異なり、クラウドサービス上でソースコードあるいはバイナリが秘匿されているプログラムは、残存している脆弱性を、多数のユーザー（特に優秀な多数のセキュリティ研究者たち）が常に環視して発見できる機会がなく、未知の脆弱性が発見されずに残存しているリスクが相当高い）、それらの多数のゼロデイ脆弱性がサイバー攻撃者（国家レベルの高度なサイバー攻撃者は、各インフラ企業で秘匿されている非公開情報を盗み出し、これに基づきサイバー攻撃を企画することができるので、クラウド事業者がプログラムを秘匿することは、これらの能力の高いサイバー攻撃者を利する結果となる）によって悪用される前に修正される機会が、少なくともバイナリが公衆に提供される伝統的なソフトウェアと比較して、非常に乏しく、危険性が高い。これは、AI に限らず、パブリッククラウド特有の未解決問題である。しかし、個人情報が一極集中する AI サービスでは、扱うデータの価値が際立って高いので、危険性はますます高くなる。

OpenAI の依存先の各クラウドサービス単体でみたとき、仮にそれぞれの脆弱性の悪用可能性が低くても、多数合わせて考えれば、全体として、悪用可能性はかなり高くなってしまふ。サイバー攻撃者としては、そのうち、1 つの脆弱性だけを突けば、足りるからである。加えて、これらのサービスをつなぎあわせてうまくセキュリティを実現する接着剂的システムの部分は OpenAI 社のプログラマ等が作成しているとみられるが、異なる設計思想に基づいて、かつ次々に仕様・実装・挙動が変化してしまうばらばらの外部の多数のクラウド型サービスに合わせた自基盤のプログラム等の修正は、とても大変な作業であり、過失による脆弱性も発生しやすい作業である。すなわち、現状の OpenAI 社のシステムは、現実世界の建物の比喻でいうと、別々の時期や設計者（業者）によって建てられた多数の建物や廊下をつなぎあわせて 1 つに見せている建て増し旅館のような構造となっており、しかもその大部分が他人がそれぞれ管理し別々の時期に増築・メンテナンスをする、賃貸の建物群なのである。この場合の弱点は、建物・廊下間の接続部分にも生じる。そして、サイバー攻撃者にとっては、大量のユーザーからの魅力的な秘密データが一極集中しているサービスは、最も魅力的な攻撃ターゲットとなる。OpenAI 社のサービスとして単体でみても、あるいは上記の（ア）～（ウ）のような各クラウドサービスをみても、非常に人気のサービスとなっていることから、OpenAI のシステムや（ア）～（ウ）のシステムには、極めて重要な機密データが全世界から一極集中して集まっているといえる。これらの人気サービスは、大規模な非合法的商業レベルの、あるいは国家レベルのサイバー攻撃者や諜報機関からみれば、少ない攻撃回数

で大量のデータを奪取できる魅力が高いため、サイバー攻撃として狙われる頻度・回数などの量と、攻撃者の質・能力は、各段に高くなってしまふ（サイバー攻撃者の視点における費用対効果が高い）。他方で、サイバー攻撃を防衛する側の能力には、技術上の限度がある。この結果、一極集中型 AI サービスやクラウドサービスのセキュリティ防衛能力は、一極集中の度合いが増せば増すほど、また、外部クラウドサービスへの内部的呼出関係の依存が増えれば増えるほど、それに応じて、投資される攻撃コストに対比して相対的に、低い水準に下がってしまうのである。これが、現代における OpenAI に代表されるクラウド的な一極集中型 AI システムのセキュリティにおける理論上の限界であり、いかにしてこれを解決するかは、AI を活用して個人情報进行分析したいと考える際に、個人情報保護法を確実に遵守しなければならない、誠実な多数の日本ユーザー企業各社のコンプライアンス上の極めて重要な問題である。

そこで、日本ユーザー企業各社の願いである、OpenAI のような AI 処理単体でみた場合に優れた性能を有する AI サービスにたいして生じてしまっているクラウド一極集中問題によるセキュリティの低下を、根本的に解決するための方法を考えてみよう。根本的な解決法としては、① 一極集中型の単一システムや単一クラウドの利用を避け、顧客が自ら AI コンピュータや GPU、ストレージを所有管理し、自らのコンピュータ上で AI プログラムを動作させる、② どうしてもパブリッククラウド型 AI サービスを利用したいのであれば、暗号技術を用いたユーザー毎の個別の機密コンピューティングを実現し、その上で AI プログラムを動作させる、の 2 つがある。だが、① は OpenAI のようなビジネスモデル（AI の学習・推論プログラムや構築方法のノウハウを、できるだけ長い間、少数人数だけが知る秘密にしておくことによる、排他性・希少性の追求）に適合しない（すくなくともバイナリプログラムを頒布する必要があり、リバースエンジニアリングが容易に可能となってしまう）。② についても、ユーザーがクラウド上の計算資源を含めた領域の支配管理権を有する必要がある、ユーザーが管理支配を行なうためにはユーザーがそのプログラムを監理しなければならない、やはりバイナリレベルでもユーザーにプログラムを開示しなければならないから、OpenAI のようなビジネスモデルに適合しない。そのため、OpenAI のような、プログラムが秘匿された一極集中クラウド型 AI サービスを利用しようとする場合、実現されるセキュリティレベルには、原理的に、かなり低い限界が生じてしまうといえる。すると、ユーザー企業の側は、データ漏えい時の莫大な賠償金額を肩代わりしてもらえる多額の保険に入る必要があるが、扱う情報が機微であればある程、前記のとおり超高額な損害賠償責任を負うリスクが高くなることから、その保険料が、AI の利用料と比べても、相当高くなってしまいかも知れない。そして、なにより重要なことは、保険では根本的な問題は解決されないという点である。AI 処理対象対象である各個人の内面に深く関わる個人情報が大規模に漏えいした際の、その損傷は、原状回復が不可能であり、金銭では補償不能である。これが、現在のクラウド型一極集中 AI に起因する個人情報処理の限界である。この問題は、IT 保険ではなく、IT 技術でのみ、解決が可能である。

われわれ日本人、特に日本において AI 技術による大きな利益を手に入れたと考えている企業人や政府関係者や政治家は、技術者も、経営者も、この部分に、おおいに注目すべきである。ここに、われわれの今後数十年の高い収益と国際競争力の

回復、ひいてはそれによる国民福祉を実現するための最大のヒントが隠されている。前述のとおり、攻撃者の視点からみた攻撃の容易性と、費用対効果の高さの観点から、今後 10 ～ 20 年間で、さまざまなクラウドベースの AI やそれらが依存しているさまざまなクラウド基盤において、セキュリティ侵害が発生し、大規模に個人データが漏えいする問題（AI・クラウド事業者による目的外利用の発覚を含む）が、時々発生するであろう。あるいは、クラウドベースの AI サービスの約款上、大変細かい例外規定が多数書かれており（あえてわかりづらく規約に埋め込む形にすれば、本文章の著者のように相当のコストをかけて細かくその規約を分析する人以外はなかなか気付かない）、それが活用される形で、あるいはその AI・クラウド事業者の所在国の政府からの強制力に名を借りた形で、AI サービスの顧客や各個人本人の意思に反して、秘かに AI・クラウド事業者がその大量の個人情報データを自己利用あるいは第三者への提供を行っていたという事案が、たびたび発生するであろう。その一部は、かなりインパクトの強い結果となり、全世界的に問題になるであろう。そうすると、すべての国のすべての企業は、企業向け AI データ処理システムあるいはサービスとして、① あるいは ② を実現できる AI システムやサービスを、ますます、切望するようになる。クラウド一極集中型には前述のような原理的なセキュリティ問題が存在するので、これを解決するためには、① または ② が必須の要素として要求されるようになる。現在の OpenAI と同等か、これを超える性能を、現在のような汎用大規模パブリッククラウド技術に依存せずに、ローカル環境あるいはコンフィデンシャル・コンピューティングをサポートしたクラウド環境で運用できるソフトウェア技術とハードウェア技術は、ほとんどの国のほとんどの企業および行政で、是非とも欲しいと、皆が考えるようになる技術である。

このように、個人情報処理が可能な程度にセキュアな AI を求める世界の風潮の形成は、21 世紀前半に、必ず発生するが、それが発生してから ① や ② を作り始めるのは、競争上、手遅れである。これには、かなり長い間のだらだらとした技術研究が必要であるためである。われわれは、先を読み、現在からその作業を、できるだけ多様な組織、できるだけ多様な人材で、互いにある程度独立し、かつ時々協力を合せて、だらだらと開始するべきである。これが、この競争に勝つ唯一の方法である。日本組織にはこのような能力、体制、資源がある上に、それを活用して良い技術を生み出すために必要な、だらだらと長期間続く技術研究の醸成にかかる時間的余裕もまだある。そのことの大切さの認識は各組織のトップの経営者の多くは自覚されており、日々そのようなメッセージを組織内に発している大企業も多くなってきた。残された問題は、各日本型組織のこれまで 20 年程度続いてしまった外注主義・計画主義的な嗜好の慣性化が原因で、過度に時間に迫られた成果を求めるという手法を、各企業内や公的組織内の技術研究の分野において、誤って選択してしまっている点である（そして、結局、長期的に収益化できる成果は何も実現されない）。これでは、日本の主権者が望んでいる、AI を含めた、デジタル本流領域（AI、クラウドコンピューティング、OS、ネットワーク、仮想化、セキュリティ等）に係る高い国際競争力を有する収益源となる技術形成はできない。だが、これは、豊富な資源や体制に乏しい競争他国の状況と比較すると、比較的軽微な内部的問題に過ぎないし、原因は慣性力であるから、ある程度の時間によって自然治癒が可能である。そのようにして元気の取り戻しに成功した既存の歴史のある日本の大企業群や日本の公的研究機関群および起業家群の技術能力・経営能力およびこれまでに

蓄積・形成してきた体制と資源と人材で、適切に長期的の技術醸成を行なうことにより、必ず、日本発の優れた AI 技術の開発は実現できる。しかも、これは、多数の日本組織から、高価値のものが、並行して、多様に実現可能である。

OpenAI 社のような少数の米国人技術者集団（各 AI 企業においては、中核部分の技術研究は、数人程度の規模である）が、苦労して開拓してくれた生成 AI のおかげで、ひとまず建て増し旅館的な突貫工事としての、多数のクラウドサービスに強度に依存してしまったシステムであったとしても、セキュリティや継続性はともかく、一応は、企業向けの価値がある AI データ処理ができるという効果が実証された。これは、たいへんにありがたいことであり、彼らに感謝すべきことである。そこで、次に必要なのは、彼らができなかったこと、すなわち前述のようなセキュリティ問題を解決する、高いセキュリティと、継続性（OpenAI のようなクラウド上の秘匿されたシステムは、通常のソフトウェアと異なり、その主体がさまざまな事情で提供をやめてしまうと動作しなくなってしまうし、いつでも提供企業技術者の意向で挙動が変わるという欠点を有するから、本格的な企業活動の中核部分では利用が困難である。これを克服し、継続性を実現するためには、AI 技術は、バイナリベースであってもよいので、ユーザーが自ら支配管理するコンピュータや GPU 上で継続的に動作可能である必要がある）の実現である。この 2 つは、前記の ① や ② により、達成される。OpenAI 社が開拓した短期的に構築された小路の後ろに敷かれる、長く使われる安全で堅牢な王道を整備し、世界中の人々がその王道を安心して通行できるようにするためには、上記の ① あるいは ② を完備した、機密データを安全に処理でき、継続性も有する AI システム群が重要である。これこそが、全世界がこれから間違いなく求めるものである。そして、われわれ日本人・日本企業・公的組織は、前述のとおり、日本人の特性に合わない短絡的・安易な戦略に誘惑されることなく、十分な時間をかければ、現有の資源・環境・人材により、必ず、この部分を開拓できる。日本は、造船・繊維・機械・鉄鋼・建設・自動車・家電・化学・半導体などの科学技術産業の大半においても、同様の方法で世界トップになってきた。まず欧米人に苦労して道を開拓してもらい、20 ～ 30 年くらいかけて、日本がその後の小路を、悠々と発展させて、世界の多数の人々が安心して歩める王道を築いてきた。日本が一旦組んだ王道の先に、欧米人が現代の IT 技術を建立した。そのころ、日本は、20 世紀末までにおおいに儲けたので、トップレベル産業国になれて満足し、今まで長い時間安眠してきた。今、ついに再度朝になり、今後ますます AI が重要となる今後の国際世界において、われわれが尊敬すべき米国の先輩方技術者群が徹夜で苦労して自主的に切り拓いてくれた上に、多少の利益を得ることの期待を実証してくれたこの AI 小路を、より勤勉・多様な多数の日本人・日本企業群が、十分な睡眠をとったのちに面倒そうに仕方無く起き上がり、長期的戦略という名目の試行錯誤的活動でゆっくりと堅牢に整備してゆき、従前の小路の弱点を解決し、はじめて世界中の人々が安心して頼ることができる大規模な王道に発展させることが、産業競争力および国際収益回復の契機となり、多数の多様な日本人・日本企業が全世界から皆ふたたび大きな収益を挙げ、国内福祉を充実させる十分な財源にもなり、再度豊かな国を実現するとともに、世界中のさまざまな人々から本心によりすすんで自由に選択される世界一の製品供給元国家としての役割を再度果たす際における、重要な鍵となるであろう。そして、それは、歴史と前例によれば、日本が十分に実現可能なことなのである。