AIの利用・開発に関する契約チェックリスト

令和7年2月

経済産業省

目次

1 チェックリスト策定の背景・目的及び想定読者

AI[1]に関連する技術は日々進化している。AI利活用の機会がさらに拡大することにより、産業におけるイノベーションの促進や社会的な課題の解決にも寄与することが期待されている。これに伴い、AI技術の利活用に関する契約を締結する場面も増加している。

経済産業省が2018年に公表し、2019年に一部改訂した「AI・データの利用に関する契約ガイドライン」（**契約ガイドライン**）[2]は、いわゆる識別系AIの分野において、AIモデル[3]（学習済みモデル）が実用化段階に入ったという当時の市場環境を前提に策定されたものである。契約ガイドラインAI編では、AIモデルの開発に焦点を当てて関連する概念を主に整理するとともに、データ編では、産業データの取扱いに関する基本的な考え方を主に整理している。

もっとも、2022年頃より、基盤モデルに代表される生成AI技術を用いたサービスが急速に普及し始め、AIモデルの開発だけでなく、その利活用の局面における契約の重要性も、以前よりさらに高まっている。

また、特に事業活動においてAI技術を用いたサービスの利活用を検討する事業者の増加が顕著である一方で、AIの技術や法務に必ずしも習熟していない事業者が導入を検討するケースも増えている。このような状況下で、AI技術を用いたサービスの利活用を行う際の契約実務に関し、以下のような懸念が挙げられている。

- AIの利活用に関する契約に伴う法的なリスクを十分に検討できていない可能性
- 保護されるべきデータや情報が予期せぬ目的に利用され、また第三者に提供される等、想定外の不利益を被る可能性

本書は、契約ガイドライン公表後におけるこのような市場環境の変化を踏まえて、AI利活用の実務になじみのない事業者を含め、我が国の事業者が実務上用いやすい形式のチェックリストを取りまとめたものである。チェックリストは、当事者間の適切な利益及びリスクの分配を目指し、ひいてはAIの利活用を促すことを目的として、特に以下の方針により策定された。

- AI技術を用いたサービスの利用者が、サービスの提供者に対して提供するデータの利用範囲や契約上のベネフィット（サービスの水準、AI生成物の利用条件等）について十分な検討を行うために必要な基礎的な知識を提供すること
- 提供されるデータの不適切な利用等を避けられるよう、利用者において、契約時にチェックするべきポイント（チェックポイント）を具体的に記載すること
- 次に示す幅広い想定読者や利用場面を念頭に置き、AI利活用の契約実務に有益な参考資料とすること

---

1. 現時点で確立した定義はないが、チェックリストでは、事業者ガイドライン（下記注4）8頁と同様、「AIシステム」（活用の過程を通じて様々なレベルの自立性をもって動作し学習する機能を有するソフトウェアを要素として含むシステム）自体又は機械学習をするソフトウェア若しくはプログラムを含む抽象的な概念を指す。

2. 経済産業省「AI・データの利用に関する契約ガイドライン 1.1 版」（2019年12月）

3. AIシステムに含まれ、学習データを用いた機械学習によって得られるモデルで、入力データに応じた予測結果を生成するものを指す。（事業者ガイドライン（下記注4）9頁）

主な想定読者	AIの知見	契約実務の知見	主な利用場面
社内法務部・ 顧問弁護士 等	AI利活用の実務経験は問わない	AI利活用のケースは未経験だが、条文レベルの検討が可能	AI利活用による競争力向上とリスク管理の両立を図る観点から、契約上の留意点を網羅的に検討
ビジネス部門 担当者 等		契約の項目立てまでは理解できるが、条文レベルの自力での提案は困難	初期的に論点を把握し、社内法務部・顧問弁護士等と連携・相談

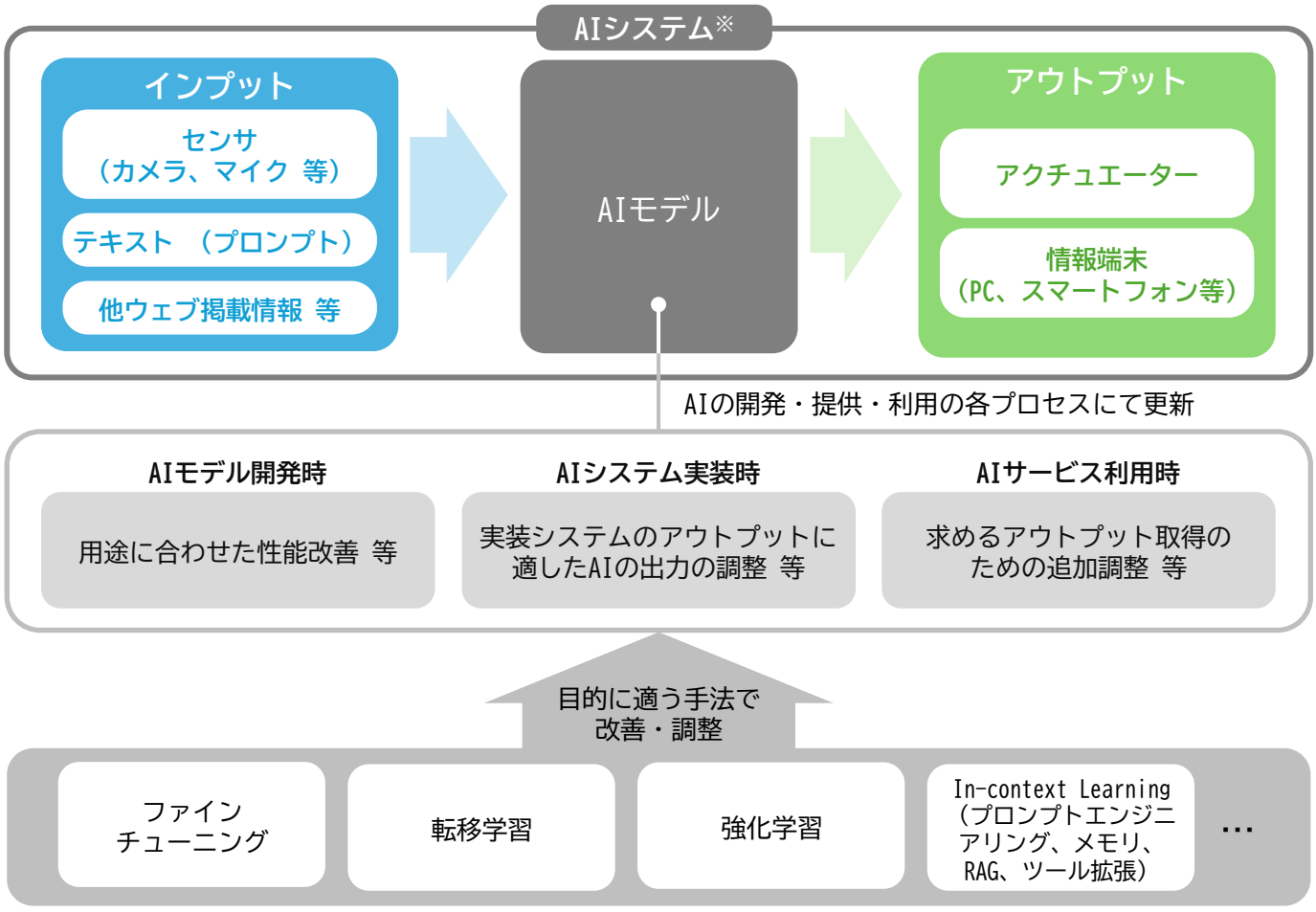
2 チェックリストの対象とするAI関連サービスのユースケース

2.1 AI利活用の流れ

2024年に公表された「AI事業者ガイドライン」（**事業者ガイドライン**）[4]では、AIモデル（学習済みモデル）を構成要素とする「AIシステム」の開発及び利用に携わる「AI開発者」「AI提供者」「AI利用者」の各当事者の役割が整理されており、チェックリストも、その整理におおむね依拠している。

チェックリストが対象とする「AIシステム」は次のとおりである（図1）。

図1　AIシステム概要

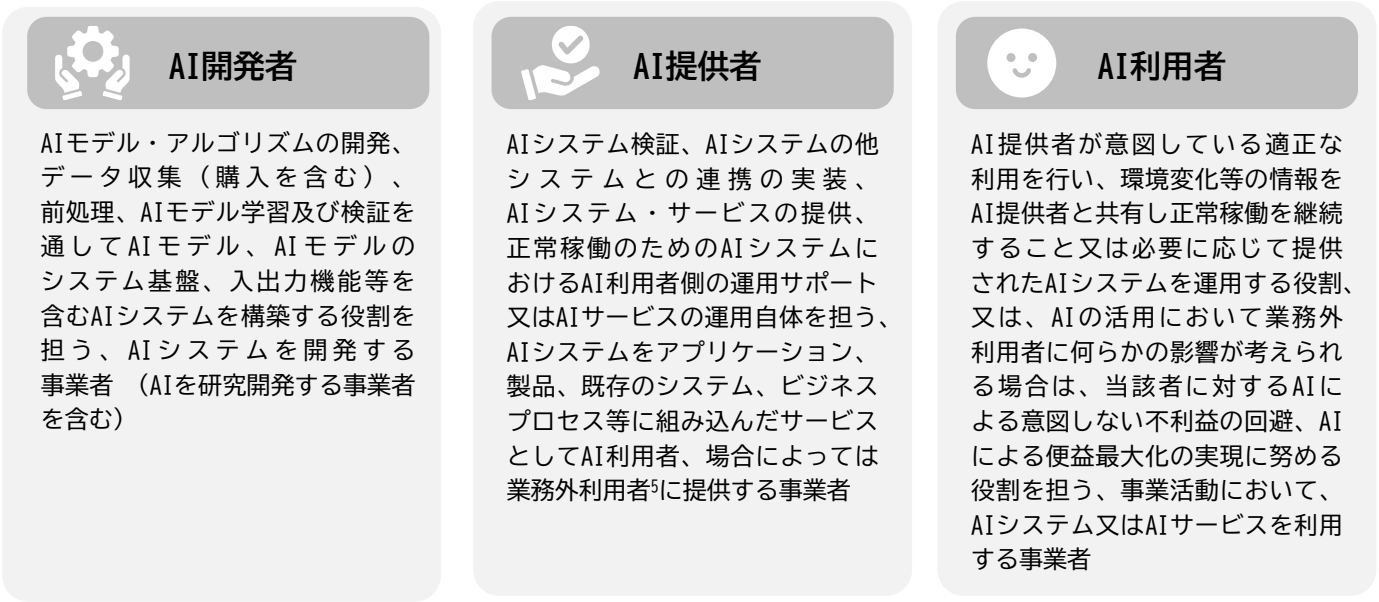


※AIモデル以外のサブシステムや別のAIモデルが並列稼働・連携することもある　　出典： 事業者ガイドライン別添（付属資料） 6頁

4. 総務省、経済産業省「AI事業者ガイドライン（第1.01版）」（2024年11月22日）

また、チェックリストでは「AI開発者」「AI提供者」「AI利用者」を次の意味で用いる（図2）。

図2　各当事者の定義



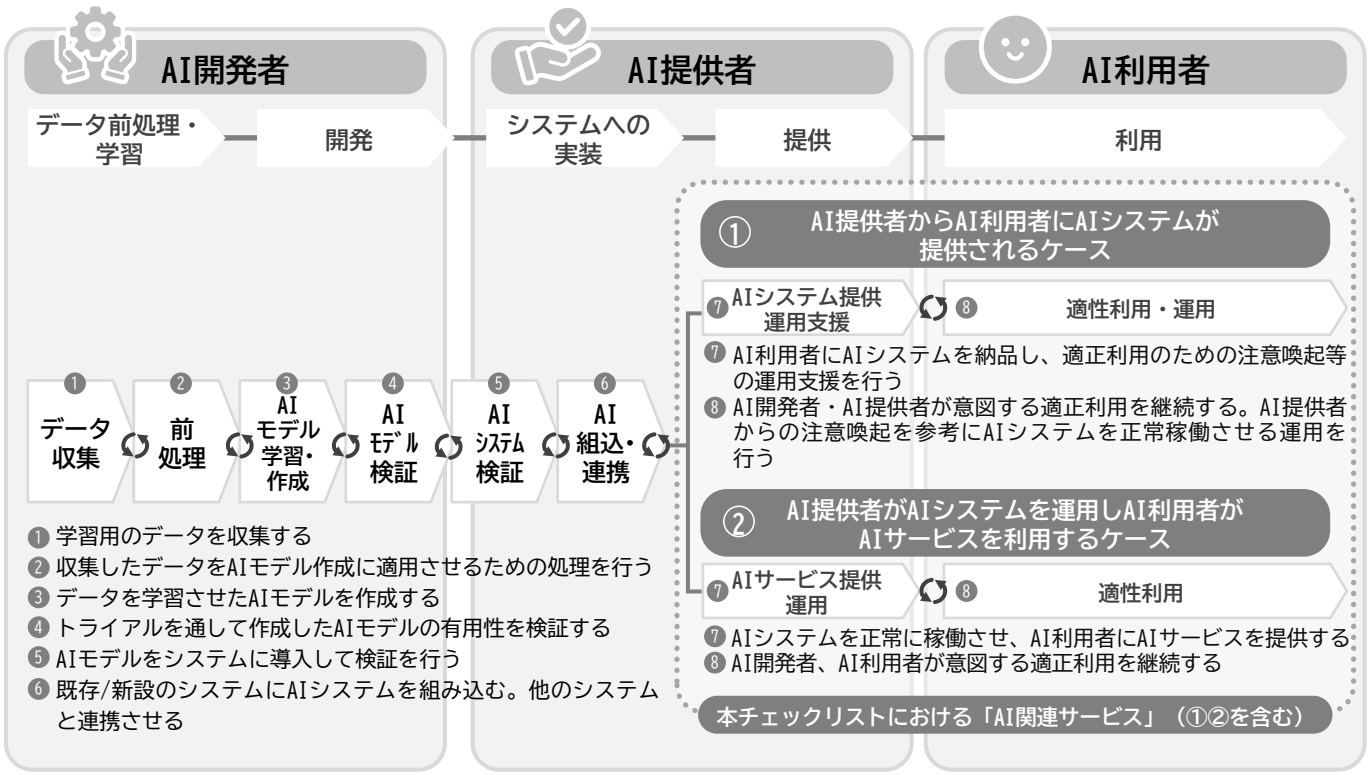
出典：事業者ガイドライン5頁

加えて、事業者ガイドラインでは、AIシステムの開発から利用に至るまでの一連の流れを整理した上で、①「AI提供者からAI利用者にAIシステムが提供されるケース」（**システム提供型**）と、②「AI提供者がAIシステムを運用しAI利用者がAIサービス[6]を利用するケース」（**サービス提供型**）が区別されている（図3）。チェックリストでは、これら①②を総称して、「**AI関連サービス**」と呼ぶことがある。②のみを指すものではない点に留意されたい。

5. 事業者ガイドライン上、「AI利用者」は全てのユーザを意味する概念ではないことには注意が必要である。「業務外利用者（事業活動以外でAIを利用する者又はAIを直接事業で利用せずにAIシステム・サービスの便益を享受する、場合によっては損失を被る者）」は、AI利用者に該当しない（事業者ガイドライン4頁）。もっとも、チェックリストは、事業者によるAI利活用の場面を対象としているため、「AI利用者」に該当するケースがほとんどであると考えられる。

6. AIシステムを用いた役務を指す。AI利用者への価値提供の全般を指しており、AIサービスの提供・運営は、AIシステムの構成技術に限らず、人間によるモニタリング、ステークホルダーとの適切なコミュニケーション等の非技術的アプローチも連携した形で実施される。（事業者ガイドライン9頁）

図3　AIシステムの開発及び利用に携わる各当事者の役割とAI関連サービス



出典：事業者ガイドライン6頁

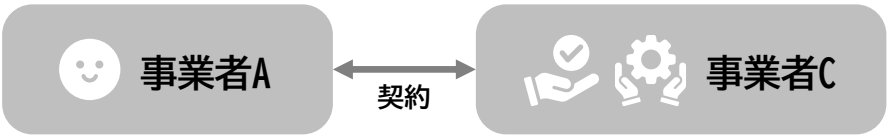
2.2 主なAIユースケースと契約類型

チェックリストでは、事業者ガイドラインの整理を前提に、サービス提供型に相当する**【類型1：汎用的AIサービス利用型】**、システム提供型に相当する**【類型3：新規開発型】**、そして、その中間に位置する**【類型2：カスタマイズ型】**の3つのAI関連サービスのユースケース類型を想定する。なお、下記のユースケース例は一例であり、これらに限られるものではない。

【類型1：汎用的AIサービス利用型】
事業者A（AI利用者）が、事業者C（AI開発者・AI提供者）が提供する汎用的AIサービスを利用するケース。

ユースケース例
小売事業者・製造事業者・サービス事業者A（AI利用者）が、マーケティングの一環で、顧客の来店・購入履歴（氏名・年齢等の情報や、実際に購入した商品・サービスの履歴が含まれたもの）を、大規模言語モデルを用いたAIサービスのプロンプトとして提供し、嗜好や注意点の分析についてのアウトプットを求めるために、事業者C（AI開発者・AI提供者）と契約する。

図4　汎用的AIサービス利用型



【類型2：カスタマイズ型】
事業者A（AI利用者）が、事業者B（AI提供者）が事業者A向けに改良・調整したAIサービス（カスタマイズサービス）を利用するケース。カスタマイズサービスは、事業者C（AI開発者・AI提供者）が開発し、提供する汎用的AIサービスに対して、事業者Bが開発した付加的な機能（非AIモデル）を組み合わせたものである。

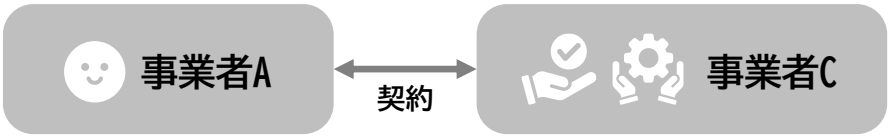
ユースケース例
小売事業者・製造事業者・サービス事業者A（AI利用者）が、ユーザエクスペリエンス改善のため、AIチャットボットサービスの提供事業者B（AI提供者）に対して、自社の業態や製品・サービスに特化したカスタマイズサービスの提供を求める。この際、提供事業者は、汎用的AIサービスの提供事業者C（AI開発者・AI提供者）との間の契約に基づき基盤モデルを利用し、モジュールやデータベース等を新規に開発する。

図5　カスタマイズ型

【類型3：新規開発型】
事業者A（AI利用者）が、事業者C（AI開発者・AI提供者）と提携して独自のAIシステムを開発・利用するケース。

ユースケース例
製造事業者A（AI利用者）が、自社製品の制御プログラムや稼働データを基に、製品の異常を早期に検知するためのシステムを開発事業者C（AI開発者・AI提供者）と提携して開発・利用する。

図6　新規開発型



チェックリストでは、これらのAI利活用の場面で通常取り扱われる契約条件について、チェックポイントを抽出・整理する。具体的には、AIシステムの開発を伴わない既存のAIサービスを利用する契約類型（**利用型契約**）と、何らかのソフトウェア、データベース、モジュールやシステムの開発を伴う契約類型（**開発型契約**）が想定される。その大まかな特色は次のとおりである。

利用型契約：
【類型1：汎用的AIサービス利用型】が想定する汎用的AIサービスを利用する契約

- 生成AIサービスに代表される幅広い利用者への汎用的AIサービスの提供が想定されており、その契約における条項が広く検討対象となる。

開発型契約：
【類型2：カスタマイズ型】や【類型3：新規開発型】等の開発が伴う契約

- 新たなソフトウェアやデータベース、モジュールやシステム等の開発要素が加わる点が、利用型契約との違いであるが、特有の要素は必ずしも多くない。したがって、汎用的AIサービス利用契約の一般的な条項に加え、開発型契約としての要素や留意事項を必要に応じて加味することで、各類型における主な検討対象となる契約条項がおおむねカバーされると考えられる。

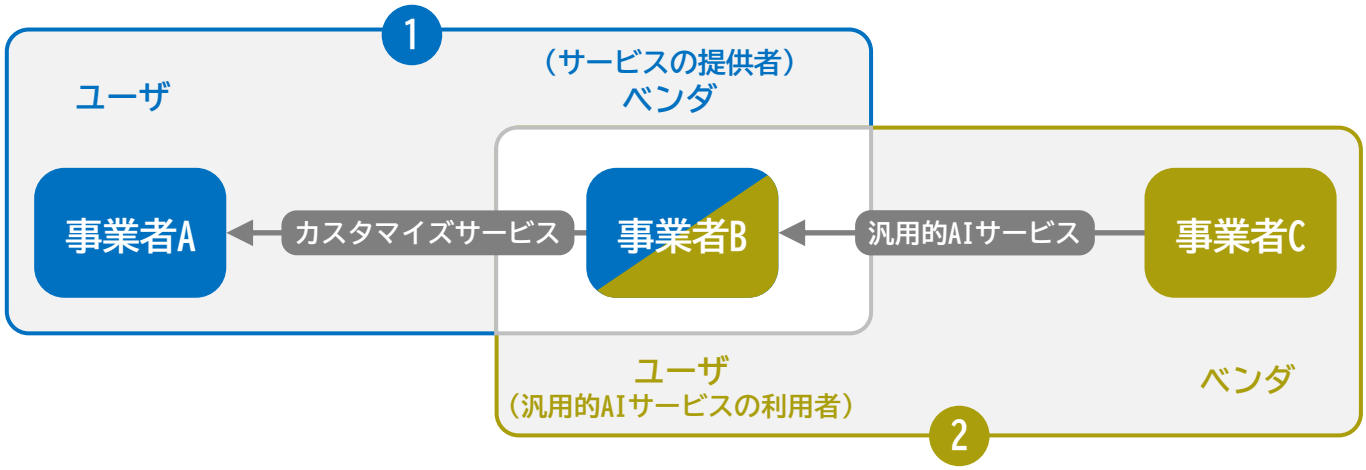
3 チェックリスト

3.1 チェックリストの対象者及び読み方

上記のようなユースケースを想定するに当たり留意すべき点として、契約上、AI開発者・AI提供者・AI利用者が果たす役割はAI関連サービスの種別に応じて異なり得ることが挙げられる。

例えば、**【類型2：カスタマイズ型】**において提供されるカスタマイズサービスは、他者が提供する汎用的AIサービスを組み込んだサービスである場面を想定している。カスタマイズサービスを提供する事業者B（AI提供者）は、①カスタマイズサービスの利用者である事業者A（AI利用者）との関係ではサービスの提供者（ベンダ）として関与するが、②汎用的AIサービスを提供する事業者C（AI開発者・AI提供者）との関係では、汎用的AIサービスの利用者（ユーザ）になる（図7）。

図7　カスタマイズ型における主体の立場の入れ替わり



したがって、チェックリストの用語上、AI関連サービスを提供する者を「**ベンダ**」、これらを利用する者を「**ユーザ**」と定義する[7]。

チェックリスト上、幾つかの項目にはアイコンが付されており、これらの項目については、チェックリストを活用する上での留意点（下記4参照）においてより詳細な留意事項を解説しているため、参照されたい。なお、上記2.2に記載のとおり、チェックリストは利用型契約と開発型契約の両方を対象とするが、利用型契約を検討するユーザは、開発型契約に関連する項目（チェックリスト上、 アイコンが付された項目）を参照せずとも、主な契約条件をひととおり検討することが可能である。

インプット提供に関する留意点（下記4.2参照）
開発型に関する留意点（下記4.3参照）
個人情報保護法に関する留意点（下記4.4参照）
セキュリティに関する留意点（下記4.5参照）

7. AI関連サービスの提供を受けるエンドユーザ（AI利用者）はもちろんのこと、エンドユーザに対してサービスを提供するAI提供者も、他の事業者の基盤モデル等を利用する際には、「ユーザ」としてチェックリストを参照することが可能である。なお、上記2.1で述べたとおり、AI関連サービスには、AIシステムを開発して提供することも含まれる。

3.2 チェックリストの対象となる条項

チェックリストは、AI関連サービスの利用に際して、ユーザがベンダに対し「**インプット（A）**」を提供し、ベンダがサービス内容に応じた「**アウトプット（B）**」を出力・提供する場面を想定している。ベンダがユーザから提供されたインプットを用いて、アウトプット以外の処理成果（「**インプット処理成果（A-6）**」）を創出することや、ユーザがアウトプットを処理することにより何らかの処理成果（「**アウトプット処理成果（B-6）**」）を得ることも想定される。

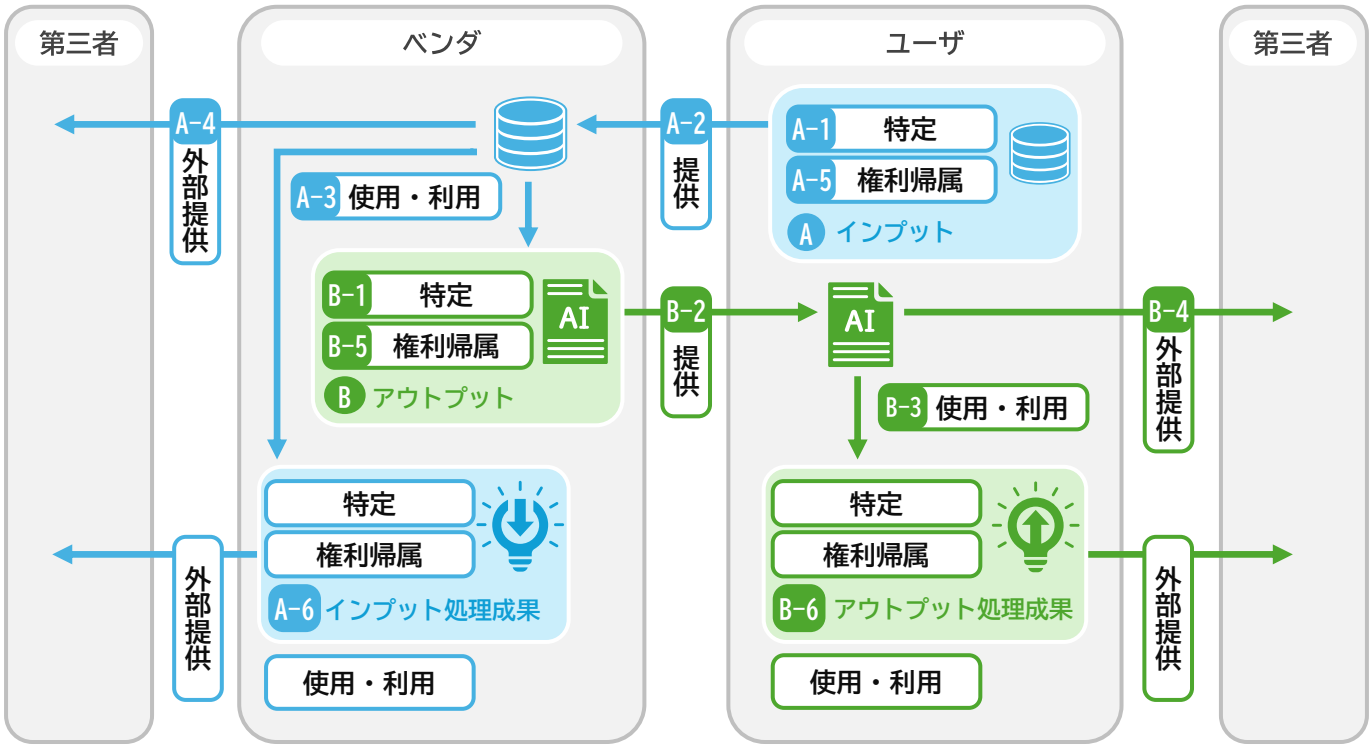
- **インプット（A）**：プロンプト、学習用の生データ　等
- **アウトプット（B）**：分析結果・コンテンツ等のAI生成物、AIシステム等の成果物　等
- **インプット処理成果（A-6）**：学習用データ、中間生成物、派生的知的財産　等
- **アウトプット処理成果（B-6）**：AI関連サービスが出力するコンテンツを自ら加工したもの　等

これらのAI関連サービスに関連する情報の取扱いに関するルールをチェックする場合、一般論としては、インプット及びアウトプットに関連して次の各点をチェックすることが望ましい（図8）。

- 契約の対象となる情報や成果物を「**特定（A-1、B-1）**」することが重要である。上記の想定の下では、インプット及びアウトプットとして具体的に何を想定するかが重要である。
- インプットを提供する立場からは、相手方への「**提供（A-2）**」に関する条項、インプットの「**使用・利用（A-3）**」に関する条項（使用・利用に加えて、管理や消去等も対象となる）、そして、相手方から自身以外の者[8]への「**外部提供（A-4）**」に関する条項をチェックすれば、相手方によるインプットの取扱いをおおむねチェックできる。
- アウトプットを受け取る立場からは、自身への「**提供（B-2）**」に関する条項、アウトプットの「**使用・利用（B-3）**」に関する条項（使用・利用に加えて、管理や消去等も対象となる）、自身から相手方以外の者への「**外部提供（B-4）**」に関する条項をチェックすれば、アウトプットの取扱い時の留意事項をおおむねチェックできる。
- 対象となる情報が知的財産権の対象である場合等、インプットやアウトプットに何らかの権利が観念できるならば、「**帰属（A-5、B-5）**」に関する条項もチェックすることが特に望ましい。
- 「**インプット処理成果（A-6）**」、「**アウトプット処理成果（B-6）**」についても、インプット及びアウトプットに準じて、その取扱いをチェックすることが重要である。

8. 図8には示していないものの、ベンダがユーザの求めに応じて、ユーザが提供したインプットを提供する場合も外部提供の一例として想定される。

図8　チェックリストの対象となる条項



チェックリストの対象となる条項に関する留意点は以下のとおりである。

- チェックリストでは、AI利活用に関する契約のうち、データの適切な利用とリスク分配の観点から特に留意すべきと思われる条項を主に取り上げている。しかし、リスク判断の観点からは、取り上げられていない条項についても、十分に検討することが望ましい。典型的には、AI関連サービス等に関する保証・補償条項、責任限定条項、解除条項、準拠法・紛争解決条項等が挙げられる。
- チェックリストは国内法に準拠した内容とし、外国法についての情報提供を意図したものではない。ただし、チェックポイントの検討に際しては、外国法準拠の場合であっても確認することが有益な内容となるように配慮している。
- 特に利用型契約に顕著であるが、ベンダが提供する契約の構成や規定・表現ぶりは各社各様である。そのため、チェックリストでは、具体的な条項例を特定するのではなく、その内容面から特に検討が必要と思われる条項についてチェックポイントを設けている。

AI利活用チェックリスト インプット

インプット提供に関する留意点（下記4.2参照）
開発型に関する留意点（下記4.3参照）
個人情報保護法に関する留意点（下記4.4参照）
セキュリティに関する留意点（下記4.5参照）

A-1 特定

A-1-1 定義｜インプットの定義を定める条項

チェックポイント

- ☐ インプットの定義は、ユーザがベンダに対し提供する情報のうち、契約上保護することが必要な情報を含んでいるか
- ☐ インプットの定義に疑義はないか
- ☐ ユーザのサービス利用目的に照らして、上記内容は許容できるか

事実上取り得る対応（契約締結断念を除く）

- 提供情報がインプットの定義に合致するかを、情報提供の前に確認する
- インプットの定義に該当しない情報は、ベンダが自由に利用可能であることを前提に、不必要な情報は提供しない

備　考

- この条項により契約による規律の対象となるインプットの範囲が定まる。インプットの定義に合致しない場合、適用法令による制限がない限り、ベンダがインプットを自由に利用できる可能性がある。
- ユーザからベンダに提供する情報は、「秘密情報」「インプット」「技術情報」「ノウハウ」「フィードバック」「プロンプト」等と呼ばれることがある。

A-2 ベンダへの提供

A-2-1 提供義務・条件 ｜ユーザがベンダに対してインプットを提供する義務の有無、及びその内容を定める条項

チェックポイント

- ☐ ユーザがベンダに対し、インプットを提供する義務を負うか
- ☐ ユーザの提供義務がある場合、いかなる提供条件（提供時期、頻度、態様その他の条件）が課せられるか
- ☐ ユーザがベンダに対し、提供するインプットの内容（性質、量、粒度その他の内容）について、満たすべき条件があるか
- ☐ ユーザのサービス利用目的に照らして、上記内容は許容できるか

事実上取り得る対応（契約締結断念を除く）

- 契約の定めの有無にかかわらず、適用法令に明白に反する情報の提供は避ける
- 他者との契約に抵触し得る情報や自社の秘密情報等を提供する場合、その許容性については慎重に検討する

備　考

- 開発型契約で定められることがあり、利用型契約で定められることは必ずしも多くない。

インプット提供に関する留意点（下記4.2参照）
開発型に関する留意点（下記4.3参照）
個人情報保護法に関する留意点（下記4.4参照）
セキュリティに関する留意点（下記4.5参照）

A-2-2 保証・情報提供｜ベンダがユーザに対して インプットに対する一定の保証・情報提供を求める条項

チェックポイント

- ☐ ユーザがベンダに対し、インプットに関する保証・情報提供をする義務を負うか
- ☐ ユーザによる保証・情報提供が求められる場合、どのような保証・情報提供が求められるか（知的財産権の非侵害、適用法令遵守等を超える保証等を求められるか）
- ☐ 保証・情報提供義務に違反した場合、どのような効果が生じるか
- ☐ ユーザのサービス利用目的に照らして、上記内容は許容できるか

事実上取り得る対応（契約締結断念を除く）

- 保証・情報提供義務を遵守できない情報は提供しない
- 保証・情報提供義務を遵守するため、提供情報の収集等の過程から取扱体制を再検討する（必要に応じて同意取得等のクリアランスを確保する）

備　考

- 第三者の知的財産権の非侵害や個人情報保護法等の適用法令の遵守に関する保証が求められることが少なくない。
- 契約上、一定の仕様が合意される場合には、その内容を充足することが求められる場合がある。

インプット提供に関する留意点（下記4.2参照）
開発型に関する留意点（下記4.3参照）
個人情報保護法に関する留意点（下記4.4参照）
セキュリティに関する留意点（下記4.5参照）

A-3 使用・利用

A-3-1 利用目的｜ベンダによるインプットの利用目的を定める条項

チェックポイント

- ☐ インプットの利用目的が定められているか
- ☐ ユーザのサービス利用目的に照らして、上記内容は許容できるか

事実上取り得る対応（契約締結断念を除く）

- ベンダによるサービス提供目的以外の利用の可能性がある場合、不必要な情報を提供しない。特にベンダが自己の学習にデータを用いる旨の定めがある場合、そのような利用が許容可能かは慎重な判断を要する
- 個人データの提供が伴う場合、ベンダによる自己目的利用や突合が認められる場合には委託として整理できず第三者提供に該当し、本人の同意が必要となる可能性があることを踏まえて、個人データの取扱いスキームを整理する（下記4.4参照）

備　考

- 利用条件で目的外利用禁止義務が定められる場合、利用条件の範囲が明確にされることになる。

A-3-2 利用条件｜ベンダによるインプットの利用条件を定める条項

チェックポイント

- ☐ ベンダによるインプットのサービス提供目的以外の利用が認められているか
- ☐ ベンダによる利用が認められる場合、どのような利用条件（利用目的、利用範囲、対価の有無、その他の条件）が課せられているか。特に自社技術開発や学習目的等のサービス提供目的以外の目的で利用することが許容されているか
- ☐ ユーザのサービス利用目的に照らして、上記内容は許容できるか

事実上取り得る対応（契約締結断念を除く）

- A-3-1を参照

備　考

- 例えば、ベンダは、AI関連サービスの提供目的以外の目的でインプットを利用しないことを目的外利用禁止義務として定めることが少なくない。

インプット提供に関する留意点（下記4.2参照）
開発型に関する留意点（下記4.3参照）
個人情報保護法に関する留意点（下記4.4参照）
セキュリティに関する留意点（下記4.5参照）

A-3-3 管理・セキュリティ｜ベンダによるインプットの管理・セキュリティ体制（セキュリティ水準を含む）を定める条項

チェックポイント

- ☐ ベンダがインプットを管理する義務を負うか
- ☐ ベンダが管理義務を負う場合、いかなる水準の管理が求められるか
- ☐ ベンダによる管理体制について、ユーザによる監査・情報提供依頼が認められるか
- ☐ ユーザのサービス利用目的に照らして、上記内容は許容できるか

事実上取り得る対応（契約締結断念を除く）

- 管理体制・セキュリティ体制が十分な水準にない場合、不必要な情報は提供しない
- 個人データの委託を伴う場合、ベンダに及ぼすことが可能な監督権限が、委託として処理するために十分な水準にあるかを検討する（水準を満たさない場合には第三者提供等として処理することを検討する。）。また、外国への個人データの移転が伴う場合、個人情報保護法上の「提供」の有無にかかわらず保有個人データに関する情報提供等が必要になり得ることに留意する（下記4.4参照）
- 個人情報の提供を伴う場合、ベンダによる個人情報の漏洩が生じた際はユーザによる監督機関への報告義務等が課せられる場合があるため、特に注意する（下記4.4参照）

備　考

- 契約で明示されていない管理水準であっても、業界水準に照らして体制構築義務が黙示の義務を構成する可能性がある（下記4.5参照）。

インプット提供に関する留意点（下記4.2参照）
開発型に関する留意点（下記4.3参照）
個人情報保護法に関する留意点（下記4.4参照）
セキュリティに関する留意点（下記4.5参照）

A-3-4 保持期間・消去｜ベンダによるインプットの保持期間及び消去義務の有無を定める条項

チェックポイント

- ☐ ベンダがインプットを保持可能な期間はどの程度か
- ☐ 保持期間が完了した場合にベンダがどのような対応をするか
- ☐ ベンダが、ユーザが求める場合や、契約期間の終了時に、インプットの削除義務を負うか
- ☐ ベンダが削除の履践を証明する書類等の発行義務を負うか（主に秘密情報の場合）
- ☐ ユーザのサービス利用目的に照らして、上記内容は許容できるか

事実上取り得る対応（契約締結断念を除く）

- 適用法令上、ベンダの削除義務が求められている場合には、契約外の権利行使として削除を求める

備　考

- 適用法令によっては、取得から一定期間が経過した場合、又は利用目的を達成したこと等を理由に取扱いの必要性がなくなった場合、削除義務や削除の努力義務が課せられている場合がある。

A-4 外部提供

A-4-1 ユーザへの提供｜ベンダがインプットをユーザに対して提供する義務を定める条項

チェックポイント

- ☐ ベンダがユーザに対し、インプットを提供する義務があるか
- ☐ ベンダによるインプットの提供義務がある場合、どのような提供条件が課せられているか（提供対象の制限の有無や、ユーザによる対価の支払いの有無や、提供可能時期、回数制限等）
- ☐ ユーザのサービス利用目的に照らして、上記内容は許容できるか

事実上取り得る対応（契約締結断念を除く）

- 提供するインプットのバックアップが必要な場合、別途、自社での対応を検討する
- 適用法令に基づき、契約外の提供請求が可能な場合には、その対応も検討する

備　考

- 特に利用型契約で、契約終了やサービス切替え等の場合に定められることが想定される。
- 特定の法域では、ポータビリティの義務として位置づけられる事も想定される。

インプット提供に関する留意点（下記4.2参照）
開発型に関する留意点（下記4.3参照）
個人情報保護法に関する留意点（下記4.4参照）
セキュリティに関する留意点（下記4.5参照）

A-4-2 第三者提供｜ベンダがインプットを第三者に提供することができるか、できる場合にその条件を定める条項

チェックポイント

- ☐ ベンダがインプットを第三者に対し提供できるか
- ☐ ベンダが第三者提供できる場合、いかなる第三者提供条件（提供先、提供範囲その他の条件）が課せられているか
- ☐ ユーザのサービス利用目的に照らして、上記内容は許容できるか

事実上取り得る対応（契約締結断念を除く）

- ベンダによる第三者提供の可能性がある場合、不必要な情報は提供しない
- インプットの第三者提供が許容できない場合には、契約締結を断念することも検討する

備　考

- 秘密保持義務条項等において、例えば、ベンダがインプットを秘密として保持し、第三者に対して提供しない等の第三者提供禁止義務として定められることが想定される。

A-5 権利帰属

A-5-1 権利帰属｜インプットの権利がベンダに移転するか否かを定める条項

チェックポイント

- ☐ ベンダがインプットに関して、知的財産権等一定の権利を取得するか
- ☐ ベンダが権利を取得する場合、どのような権利取得条件（権利移転の対象、対価の有無、ライセンスの有無・内容その他の条件）があるか
- ☐ ユーザのサービス利用目的に照らして、上記内容は許容できるか

事実上取り得る対応（契約締結断念を除く）

- ベンダによる権利取得の可能性がある場合、不必要な情報を提供しない

備　考

- 一般的には、ユーザがベンダに対し、インプットの権利を移転する必要が生じる場面は限定的である。

インプット提供に関する留意点（下記4.2参照）
開発型に関する留意点（下記4.3参照）
個人情報保護法に関する留意点（下記4.4参照）
セキュリティに関する留意点（下記4.5参照）

A-6 インプット処理成果

A-6-1 特定｜インプットの処理成果のうち、アウトプット以外のもので契約上規律の対象とするものの定義を定める条項

チェックポイント

- ☐ インプット処理成果の定義は、ベンダの処理により生じる成果のうち、契約上保護することが必要な情報を含んでいるか
- ☐ インプット処理成果の定義に疑義はないか
- ☐ ユーザのサービス利用目的に照らして、上記内容は許容できるか

事実上取り得る対応（契約締結断念を除く）

- ベンダがインプット処理結果を、一定範囲で、自由に利用可能である可能性があることを前提に、不必要な情報を提供しない

備　考

- インプットに何らかの処理（加工等）を施した無体物を指し、「派生物」「派生的知的財産」「派生データ」「改良成果」等と呼ばれることもある。生データに対する学習用データセット等の中間生成物が典型的に想定される。
- インプット処理成果を契約上取扱う必要が常にあるわけではない点には留意が必要である。
- 利用型契約では、言及されることは必ずしも多くない一方、開発型契約では議論がされることがある。ベンダの技術的知見に属する処理成果の取扱いを規律することの当否は、慎重に検討する必要がある。

A-6-2 使用・利用｜インプット処理成果のベンダによる使用・利用に関する条項

A-3 使用・利用 を参照

A-6-3 外部提供｜インプット処理成果のベンダによる外部提供に関する条項

A-4 外部提供 を参照

備　考

- インプット処理成果には、ベンダの技術的知見が多分に反映されているものも含まれる。そのような場合、ユーザに当然に提供がなされるべきものではない点は留意が必要である。

A-6-4 権利帰属｜インプット処理成果の権利帰属に関する条項

A-5 権利帰属 を参照

AI利活用チェックリスト アウトプット

インプット提供に関する留意点（下記4.2参照）
開発型に関する留意点（下記4.3参照）
個人情報保護法に関する留意点（下記4.4参照）
セキュリティに関する留意点（下記4.5参照）

B-1 特定

B-1-1 定義｜アウトプットの定義を定める条項

チェックポイント

- ☐ アウトプットの定義は、ユーザのサービス利用目的を十分にカバーしているか
- ☐ アウトプットの定義に疑義はないか（開発型 特に開発型契約の場合には、開発対象が不明確となる場合が少なくないため注意）
- ☐ ユーザのサービス利用目的に照らして、上記内容は許容できるか

事実上取り得る対応（契約締結断念を除く）

- 契約上合意したアウトプットの定義・内容を踏まえ、実際の利用目的に照らして不十分である場合、別の手段による調整や補正の必要性を含めて事前に検討することが望ましい

備　考

- この条項により、契約で規律の対象となるアウトプットの範囲が定まる。
- 利用型契約では、「出力結果」「アウトプット」「コンテンツ」等呼ばれることがある。
- 開発型 ベンダからユーザに提供する情報は、開発型契約であれば「成果物」と呼ばれることがある。

B-2 ユーザへの提供

B-2-1 完成義務｜開発型 ベンダがアウトプットを完成させる義務を定める条項

チェックポイント

- ☐ ベンダがアウトプットを完成する義務を負うか
- ☐ ベンダの完成義務がある場合、どのような完成条件が課せられるのか（完成時期、検収条件等）
- ☐ ユーザのサービス利用目的に照らして、上記内容は許容できるか

事実上取り得る対応（契約締結断念を除く）

- 完成義務を負わない場合でも、ベンダは善管注意義務を負う。アウトプットの開発に際して、十分な意思疎通を試み、当事者間の期待値がずれないように調整することが望ましい
- 利用を希望する時期までに十分なアウトプットが提供されない場合の対応は、事前に検討する事が望ましい

備　考

- 開発型契約のうち、請負型契約（民法632条参照）で特に問題となる。

インプット提供に関する留意点（下記4.2参照）
開発型に関する留意点（下記4.3参照）
個人情報保護法に関する留意点（下記4.4参照）
セキュリティに関する留意点（下記4.5参照）

B-2-2　提供義務・条件｜ベンダがユーザに対し、アウトプットを提供する義務の有無及びその内容を定める条項

チェックポイント

- ☐ ベンダがユーザに対し、アウトプットを提供する義務を負うか
- ☐ ベンダの提供義務がある場合、どのような提供条件（提供時期、頻度、態様その他の条件）が課せられるか
- ☐ ベンダがユーザに対し、提供するアウトプットの内容（性質、量、粒度その他の内容）について、満たすべき条件があるか
- ☐ ユーザのサービス利用目的に照らして、上記内容は許容できるか

事実上取り得る対応（契約締結断念を除く）

- アウトプットが提供されない場合、アウトプット（又はこれを利用したサービス）のメンテナンス・運用等が十分に行えるかを、事前に検討する事が望ましい

備　考

- 開発型契約の中には、開発の成果物（アウトプット）を提供する義務が課せられない場合がある。（下記4.2参照）

B-2-3 保証・情報提供｜ユーザがベンダに対し、アウトプットに関する一定の保証を求める条項

チェックポイント

- ☐ ベンダがユーザに対し、アウトプットの保証・情報提供義務を負うか
- ☐ ベンダによる保証・情報提供が必要な場合、どのような条件による保証・情報提供が必要なのか
- ☐ 保証・情報提供違反があった場合、どのような効果が生じるか
- ☐ ユーザのサービス利用目的に照らして、上記内容は許容できるか

事実上取り得る対応（契約締結断念を除く）

- ベンダによる保証がない場合のみならず、保証がある場合であっても、機械学習の特性上、アウトプットには、不正確な情報や虚偽の情報、あるいは他者の著作権等の権利利益を侵害する情報が含まれる可能性がある。したがって、利用目的に応じて、アウトプットの正確性や適法性を適切に評価し、人による確認を行うことが必要である

備　考

- 適用法令によっては、ベンダに透明性確保の観点からアウトプット生成に関する一定の情報提供が求められる場合が想定される。
- 利用型契約では、幅広い非保証条項が設けられることがあるのに対して、開発型契約では、第三者の知的財産権の非侵害や要求された仕様への合致等が求められる場合が少なくない。ただし、請負型契約か準委任型契約かにより左右される側面がある。

インプット提供に関する留意点（下記4.2参照）
開発型に関する留意点（下記4.3参照）
個人情報保護法に関する留意点（下記4.4参照）
セキュリティに関する留意点（下記4.5参照）

B-3 使用・利用

B-3-1 利用目的｜ユーザによるアウトプットの利用目的を定める条項

チェックポイント

- ☐ アウトプットの利用目的の定めがあるか
- ☐ ユーザのサービス利用目的に照らして、上記内容は許容できるか

事実上取り得る対応（契約締結断念を除く）

- 意図しない目的外利用が発生しないよう、管理体制の構築及び社内教育等を十分に実施する

備　考

- 利用条件で目的外利用禁止義務が定められる場合、利用条件の範囲が明確にされることになる。

B-3-2 利用条件｜ユーザによるアウトプットの利用条件を定める条項

チェックポイント

- ☐ ユーザによるアウトプットの利用について、いかなる利用条件（追加的対価・プロフィットシェア、利用目的の制限、禁止的行為、利用範囲その他の条件）が課せられているか
- ☐ ユーザのサービス利用目的に照らして、上記内容は十分か

事実上取り得る対応（契約締結断念を除く）

- B-3-1を参照。

備　考

- AI関連サービスによっては、商用利用の禁止やアウトプットがAIを用いて生成されたことを表示する等の条件設定がされることがある。

B-3-3 管理・セキュリティ・消去｜ユーザによるアウトプットの管理・消去体制を定める条項

チェックポイント

- ☐ ユーザがアウトプットの管理・消去義務を負うか。負う場合その内容は何か
- ☐ ユーザのサービス利用目的に照らして、上記内容は許容できるか

事実上取り得る対応（契約締結断念を除く）

- 合意内容に照らしてアウトプットを適切に管理・消去等する

備　考

- アウトプットが形式上、ベンダの秘密情報に該当する場合等には適用されることが想定される（そのような場合でなければ一般的には想定し難い）。

インプット提供に関する留意点（下記4.2参照）
開発型に関する留意点（下記4.3参照）
個人情報保護法に関する留意点（下記4.4参照）
セキュリティに関する留意点（下記4.5参照）

B-4 外部提供

B-4-1 第三者提供｜ユーザがアウトプットを第三者に提供することができるか、できる場合にその条件を定める条項

チェックポイント

- ☐ ユーザがアウトプットを第三者に対し提供できるか
- ☐ ユーザが第三者提供できる場合、どのような第三者提供条件（提供先、提供範囲その他の条件）が課せられているか。利用型の場合には、AIを用いたサービスによるものである旨の表示をする必要があるか
- ☐ ユーザのサービス利用目的に照らして、上記内容は許容できるか

事実上取り得る対応（契約締結断念を除く）

- 意図しない第三者提供（情報漏洩を含む）が発生しないよう、管理体制の構築及び社内教育等を十分に実施する

備　考

- 秘密保持義務条項等において第三者提供禁止義務として定められる場合がある。

B-5 権利帰属

B-5-1 権利帰属｜ベンダがユーザに対し、アウトプットを提供する場合、アウトプットの権利がユーザに移転するかどうかを定める条項

チェックポイント

- ☐ ユーザがアウトプットに関して、知的財産権等、一定の権利を取得するか
- ☐ ユーザが権利を取得する場合、どのような権利取得条件（権利移転の対象、対価の有無、ライセンスの有無・内容その他の条件）があるか
- ☐ ユーザのサービス利用目的に照らして、上記内容は許容できるか

事実上取り得る対応（契約締結断念を除く）

- アウトプットに関する権利がユーザに移転しない場合、アウトプットの利用方法が限定されることを理解した上でサービスを利用する

インプット提供に関する留意点（下記4.2参照）
開発型に関する留意点（下記4.3参照）
個人情報保護法に関する留意点（下記4.4参照）
セキュリティに関する留意点（下記4.5参照）

B-6 アウトプット処理成果

B-6-1 特定｜アウトプットの処理成果のうち、契約上規律の対象とするものの定義を定める条項

チェックポイント

- ☐ アウトプットの処理成果の定義は、ユーザの処理により生じる成果のうち、契約上保護することが必要な情報を含んでいるか
- ☐ アウトプットの処理成果の定義に疑義はないか
- ☐ ユーザのサービス利用目的に照らして、上記内容は許容できるか

事実上取り得る対応（契約締結断念を除く）

- 意図しない目的外利用・第三者提供等が発生しないように、管理体制の構築及び社内教育等を十分に実施する

備　考

- アウトプットに何らかの処理（加工等）を施した無体物を指し、「派生物」「派生的知的財産」「派生データ」「改良成果」等と呼ばれることもある。
- 例えば、画像をアウトプットとして出力するAIサービスの場合には、出力画像（アウトプット）をさらにユーザが加工した画像の取扱いに関する規律の一環として定められることが想定される。

B-6-2 使用・利用｜アウトプットの処理成果のユーザによる使用・利用に関する条項

B-3 使用・利用 を参照

B-6-3 外部提供｜アウトプットの処理成果のユーザによる外部提供に関する条項

B-4 外部提供 を参照

備　考

- アウトプットそのものと異なり、ベンダへの報告義務が課せられる場合がある点には留意が必要である。

B-6-4 権利帰属｜アウトプットの処理成果の権利帰属に関する条項

B-5 権利帰属 を参照

4 チェックリストを活用する上での留意点

4.1 チェックリストを踏まえた対応

チェックリストは、AIの利活用に関する契約を締結するに際して考慮することが望ましい論点の所在を示すに留まる。**チェックリストでリスクの所在が指摘されているからといって、直ちに契約条件の是正に向けた行動を取ることや契約締結を断念することを推奨するものではない。**

契約の主たる機能には、当事者間のリスク分配があるものの、リスクはAIの利活用それ自体に内在するものであって契約文言の巧拙で完全にコントロールできるものではない。そのため、**契約上、相手方が一定のリスクに対する最終的な対応責任を負うとされる場合でも、リスクの発生自体を回避できるとは限らない。**また、自社が契約上一定のリスクを負うとされるような**必ずしも望ましくない契約条件が課せられる場合でも、リスクが発生する可能性が事業上許容可能な範囲内にある場合や、契約外の対応によってその発生可能性を事業上許容可能な範囲まで低減できる場合には、契約を締結し事業を進めることが合理的と判断される場合もある。**

チェックリストを踏まえてどのように対応することが適切であるかは、個別のユーザが置かれた具体的な事情に依拠するため、以下の各要素を含む関連する事情を総合的に考慮して判断することが必要である。

- ベンダにより提供されるAI関連サービスの内容
- 契約の形態（利用規約又は個別契約）
- 契約文言を受け入れることによるリスク
- 契約上の各義務の履行可能性
- AIの利用目的に照らした代替サービス及び代替手段の有無
- 契約交渉に必要な労力
- 契約外（実運用等）の方法によるリスク低減の可否

特に、AI関連サービスのユースケース例（上記**2.2**参照）で示したように、利用型契約と開発型契約を締結する場面において、想定されるリスクに対して取り得る対応は異なる場合がある。

利用型契約：
【類型1：汎用的AIサービス利用型】が想定する汎用的AIサービスを利用する契約

- 多数のユーザと画一的な契約を締結し、その提供等に関して想定されるリスクを一定範囲に限定することで、サービス利用料等の対価やその他の契約条件が合理的な範囲に設定されていることも想定される。そのような場合、**ユーザとしては、適用法令に反する契約条件が設定されている、あるいは著しく不利益であって受容可能性がない等の例外的な場面を除き、契約条件を所与の前提としてサービス利用に関する実運用を工夫し、AIの利活用を進めることが合理的な場合もある。**もっとも、多くのユーザが抱くであろう合理的な要望や懸念をベンダに対して伝えることは、汎用的AIサービスの場合であっても、ベンダに契約条件の見直しを促す契機になる場合もあり得る。

開発型契約：
【類型2：カスタマイズ型】や【類型3：新規開発型】等の開発が伴う契約

- ユーザとベンダとの間で、AIシステム開発に関する個別の契約交渉が行われるため、利用型契約に比べると、より柔軟に交渉がしやすい場面が想定される。そのため、交渉によって望ましい契約条件への調整を試みることも一つの選択肢となる。**特に自社の技術情報、その他の有用なデータを提供するに当たっては、情報を開示することにより得られるメリットと、開示することにより生じるデメリットとを十分に比較検討をした上で契約交渉をすることが一般的には望ましい。**ただし、例えば**【類型2：カスタマイズ型】**のように、汎用的AIサービスをカスタマイズして提供する場面では、カスタマイズサービスのベンダは汎用的AIサービスのユーザとしての位置づけも有するため、同サービス利用契約に拘束され、個別交渉においても、受容できるリスクの範囲が限定される場合も考えられる。

また、**【類型2：カスタマイズ型】**に顕著であるが、ベンダがユーザに対しAIサービスを提供するに当たり、第三者が提供する汎用的AIサービスを組み込んでいるケースも想定される。例えば、ユーザの質問に対して、生成AIを用いて自然な回答を出力するAIチャットボットサービスにおいて、回答の生成を、ベンダ以外の第三者が提供する汎用的AIサービスが担うような場合である。

このようにAIサービスの提供にベンダ以外の第三者が関与することが知れている場合には、そのような第三者がベンダを介して提供するAIサービスに関する利用規約等についても、可能な範囲でチェックリストに挙げた観点から検討を行うことが考えられる。もっとも、ベンダにおいて、自社のAIサービスに組み込んでいる他のAIサービスを提供する第三者の詳細や、そのような第三者との間の契約条件を明らかにすることが困難な場合も考えられることから、ユーザとしてどこまでの情報を収集して意思決定を行うことが合理的かは個別の状況次第であり[9]、柔軟な対応が必要となる。

9. 例えば、カスタマイズサービスの利用規約等において、ベンダが契約上の義務の一部を第三者に委託する際にユーザの同意が必要とされているようなケースでは、同意をするか否かの意思決定において、ベンダと第三者との間の契約条件等は重要な考慮要素となるため、一定の情報開示を求めることは必ずしも不合理ではないと考えられる。

4.2 インプット提供に関する留意点

AI関連サービスは、ユーザが提供したインプットに対し、アウトプットを出力・提供することを中核的な内容とするサービスである。そのため、インプット及びアウトプットの取扱いに関する契約条件は、AI関連サービスを利用するための契約締結に際して、慎重な検討を要する条項である。特に、ユーザがインプットを提供しなければアウトプットは出力・提供されないことに照らせば、インプットを提供する十分なインセンティブがユーザ側に確保されるかとの視点は重要となる。

一般論として、契約上、アウトプットのユーザによる利用可能性が制限されている場合や、インプットを提供することでユーザが大きな不利益を被る場合等には、アウトプットを得てこれを利用することによるベネフィットを、インプット提供に伴う契約上又は事実上のデメリットが上回ることが想定される。そのような状況では、ユーザが契約条件をそのまま受け入れることが難しく、インプットの提供に対して、十分なインセンティブや合理性を見いだすことができないことも想定される。インプットやアウトプットの取扱いについては、幾つかの留意事項が考えられるが、特に、次の場合には注意が必要である。

【インプットの取扱い】

- ユーザがインプットを提供する際に、対価なしでその知的財産権等をベンダに移転することが契約条件として定められている場合（**このような権利移転に、AI関連サービス提供との関連性や必要性がない場合には、一般論としては契約締結の合理性は低いと考えられる**）
- ユーザが提供するインプットが、AI関連サービスの提供を超えて利用される場合（ただし、ベンダの技術向上目的については、一概にユーザにとって不利益とまでは言えない）

【アウトプットの取扱い】

- アウトプットの商業利用を想定しているにもかかわらず、契約上そのような利用が許容されていない場合、又は制限的な義務が付されている等、事業上の利用可能性が契約上確保できない場合
- アウトプットとして、第三者の知的財産権その他の権利利益を侵害するものが出力・提供されるおそれが高い場合等、適用法令に照らして事業上の利用可能性が確保できない場合
- アウトプットにバイアスや不正確な回答が散見される等、社会的又は事業上の観点から利用が許容されない場合

したがってユーザは、インプットやアウトプットの取扱いに関する契約条件を十分に精査し、アウトプットを得ることによるベネフィットや、インプットを提供することによるリスク（特に自社が不合理なリスクを負担することにならないか）を把握した上で、その契約条件を受け入れるか否かの判断が求められる。この際、契約条件により設定されたリスク分配あるいはリスク負担を前提とした上で、インプットの提供に伴うリスクの低減策も考慮し、慎重に検討することが必要である。

特に、AI関連サービスについては、**インプットが汎用的なAI学習目的（自社のサービスの改善や改良目的の形で表現される場合がある）に利用される場合**（下記4.2.1参照）、**ユーザへのサービス提供に必要な範囲でのみAI学習目的に利用される場合**（下記4.2.2参照）、及び**インプットがAI学習目的に利用されない場合**（下記4.2.3参照）等が想定される。リスク範囲が異なるため、次の各場面に応じてインプットに含める情報範囲を検討することが有益と考えられる。

4.2.1 インプットが汎用的なAI学習目的に利用される場合

インプットが汎用的なAI学習目的に利用される場合、すなわち、自社が提供したインプットが学習等、第三者も利用するAIサービス改良のために用いられる場合、以下のリスクが想定される。一方で、一度AIモデル（学習済みモデル）に取り込まれた情報の除去は一般的には困難であり、事後的な是正措置を講じることも難しい。したがって、不必要な情報を可能な限りインプットに含めないことが基本的な対応方針であり、そのための社内体制の整備と周知徹底が重要である。

【個人情報保護法違反のリスク】

- インプットの提供が個人データの提供であると評価され、かつ、ベンダによる学習が委託（個情法27条5項1号）に当たらないと評価される場合には、法令上の例外事由に該当しない限り、本人の同意なく個人データを第三者[10]に提供することは個人情報保護法に違反するおそれがある。

【自社の機微情報流出のリスク】

- AI関連サービスに用いられる技術次第では、第三者からのアクセスやプロンプト等を通じてインプットの内容が漏洩する可能性がある。そのため、自社の秘密情報等の機微情報を提供する場合、その内容が第三者に開示されるリスクを十分に考慮する必要がある（特に、不正競争防止法上の営業秘密に該当する情報については、公知となる場合、以後の要保護性が失われる可能性がある。）。

【秘密保持義務等違反のリスク】

- 第三者との契約で秘密保持義務等の外部提供禁止義務を負う情報をインプットとして提供する場合、契約内容次第ではそのような行為が契約違反となるおそれがある（不正競争防止法上の営業秘密や限定提供データに該当する情報については、不正競争行為を構成するおそれもある。）。

10. 個人情報保護法や秘密保持契約等の情報の取扱いに関する規律では、一般的に、情報を「第三者」に提供することを禁止するルールが設けられている。インプットの提供の場面では、提供先であるベンダが「第三者」に該当するか否かが論点となるが、「第三者」の範囲は一様ではなく、各種の法令や契約ごとに異なる意義を有していることが通常であり、個別の検討を要することに留意が必要である。例えば、本文に記載のように、個人データの取扱いの委託に伴ってインプットが提供される場合、ベンダは「第三者」に該当せず（個情法27条5項1号）、個人情報保護法には違反しないと整理し得るが、秘密保持契約等においてこのような例外規定が存在しない場合には、インプットの提供が契約違反を構成し得る点に留意が必要である。

【知的財産権等の権利利益侵害のリスク】

- （学習目的利用であるかにかかわらず）第三者が知的財産権又は法的に保護された権利利益を有する情報をインプットとして提供することは、権利侵害となる可能性がある。例えば、第三者の著作物をインプットとして提供する際に、権利制限規定の適用がされない場合には、複製権や翻案権、公衆送信権等の著作権を侵害するおそれがある。

なお、チェックリストは、ベンダによる自社技術の開発目的利用自体が不適切であると評価するものではない[11]。重要なのは、適用法令を遵守した上で、ユーザが契約条件及びそれに伴うリスクを適切に認識し、アウトプットを得て利用することによるベネフィットと、インプットの提供にともなう契約上又は事実上のデメリットとを比較・判断した上で契約条件を受け入れるか、又はどのようなインプットを提供するかを決定することである。こうしたベネフィットとデメリットの比較衡量は、重要なデータを提供する場合には特に慎重に行うことが必要である。

11. ベンダの技術力が向上することでユーザが直接又は間接的にベネフィットを受ける場面も想定される。

4.2.2 ユーザへのサービス提供に必要な範囲でのみAI学習目的に利用される場合

上記4.2.1のように不特定多数のユーザのために汎用的なAI学習目的でインプットが用いられる場合とは異なり、特定のユーザが内部文書や取引情報をベンダに提供し、これらの情報を用いてAIシステムを改良・調整することで、そのようなユーザの個別のニーズに特化したアウトプットを出力するAIサービス（カスタマイズサービス）が存在する（上記**【類型2：カスタマイズ型】**参照）[12]。

カスタマイズサービスが特定のユーザに対してのみ提供される場合には、上記4.2.1に述べた幾つかのリスクは、そもそも発生しない、又は低減されていることが想定される。ただし、契約や約款に基づき例外的にベンダが第三者にインプット又は学習結果を自己使用・外部提供することを許容する規定になっている場合や、ベンダのシステムの欠陥やサイバー攻撃等によりこれらが外部に漏えいすること、ベンダが自己使用・第三者への提供禁止義務を履行せず無断使用する等のリスク自体は存在するため、提供するインプットの内容は慎重に判断し、そのための社内体制の整備や周知徹底を行うことが重要である。なお、インプットがユーザ自身へのサービス提供に必要な範囲でのみAI学習目的に利用され、他の目的で使用されず、また第三者に対して漏えい・提供されることがない環境が確保されているかは、ベンダ側の運用やセキュリティ水準に依拠するため、特に自社の機微情報をインプットに含める場合には、システムの構造やセキュリティ水準等に関して慎重な検討（下記4.5参照）を行うことが必要である。

4.2.3 インプットがAI学習目的に利用されない場合

インプットがAI学習目的に利用されない場合には、上記4.2.1に述べたリスクは、上記4.2.2の場合と比較してもより低減されていることが少なくないと考えられるものの、これらの場合と同様に、提供するインプットの内容については慎重に判断し、そのためのベンダに対する監理の徹底、社内体制の整備や周知徹底を行うことが重要となる。なお、インプットがAIサービスの改良のために使用されず、また第三者に対して漏えい・提供されることがない環境が確保されているかは、ベンダ側の運用やセキュリティ水準に依拠するため、特に自社の機微情報をインプットに含める場合には、システムの構造やセキュリティ水準等に関して慎重な検討（下記4.5参照）を行うことが必要である。

12. 4.2.2が想定する場面とは異なり、例えば、医療業界に属するユーザからのインプットを用いて同業界で広く使えるようなAI関連サービスを開発し、当該AI関連サービスが複数のユーザに対して広く提供されるケースもある。このような場合は、改良されたAI関連サービスが当該ユーザ以外の第三者に対しても提供されるケース（上記4.2.1）に当たる。

4.3 開発型に関する留意点

ユーザがベンダに対し、AIシステム、あるいはその利用に必要なモジュールの全部又は一部の開発を委託する場合、特に以下の点に注意を要する。

4.3.1 インプットの取扱い

開発型契約では、利用型契約（特に定型約款に基づき契約が成立する場合）と比較して、インプットやインプット処理成果の利用条件が契約交渉の重要な検討事項になることが少なくない。典型的には、ベンダがAI関連サービスの提供目的を超えて自社技術の開発目的にインプットを利用することを希望する場合、そもそもそのような利用を認めるのか、認める場合の具体的な条件（利用可能範囲及び利用禁止範囲）を検討する必要がある（インプットの提供に伴うリスクは上記4.2参照）。

4.3.2 アウトプットの取扱い

アウトプットの取扱いは、【契約の性質決定】、【AIシステムの開発に関する留意点】及び【権利帰属/利用条件】の3点について留意する必要がある。

【契約の性質決定】

- 開発型契約の契約交渉に際しては、その契約の性質を、委任事務の遂行を目的する準委任契約（民法656条・643条）と、仕事の完成を目的とする請負契約（民法632条）とするかが、重要な交渉事項とされることがある。両類型には幾つかの違いがあるが、準委任契約と理解される場合にはベンダは善管注意義務（民法644条）を負うに留まる一方、請負契約と理解される場合には仕事の完成義務（民法632条）及び契約不適合責任（民法559条・562条から564条）を負う点は、一般的に重要な相違点である。
- ただし、これらの民法上の典型契約を前提とする契約の性質の区分は、あくまでも当事者間で合意がない場合の補充的なルールを定めるにすぎない。そのため、開発型契約が準委任契約か請負契約のどちらに分類されるかを抽象的に議論することの妥当性は検討が必要である。例えば、交渉対象の開発型契約が、準委任契約に分類されたとしても、ベンダは善管注意義務を負い、一定の水準に達しない開発が行われる場合には債務不履行責任を問われ得る点に変わりはない。
- **対象となる開発型契約が準委任契約であるか、それとも請負契約は相対的なものであり、むしろユーザがベンダに対して、成果の内容や水準をどの程度求めるかが重要な論点となる場合が少なくない点に留意が必要である。**

【AIシステムの開発に関する留意点】

- 契約ガイドラインAI編は、典型的には、AIモデル（学習済みモデル）を開発する場面を想定し、その契約条件に関する留意点を説明している。特にAI編では、AIモデルが、学習用データセットに基づく帰納的な手法により開発されるという技術的な背景を踏まえ、AIモデルに関する完成義務の設定や性能保証が必ずしも容易でない点を指摘している。AI編で述べられた事項は、開発型契約がAIモデルを直接の開発対象とする際、特に**【類型3：新規開発型】**の場面において、依然として妥当である。
- 他方で、AIモデルそのものではなく、AIモデルを含むAIシステムを開発する場合には、AIモデルの出力等の不確実性を十分に考慮したシステム設計・開発が求められることも想定される。このような場合、開発対象であるAIシステムの実現について、ベンダが一定の担保責任を負うことが合理的な場面も考えられる。ただし、**【類型2：カスタマイズ型】**のように、ユーザとベンダの間でAIシステムの運用に関する継続的な契約関係が存在する場合、一つの契約によりリスク分配を図ることが適切であるか、あるいは可能であるかについては、十分に考慮することが望ましい。特に開発型契約が締結される時点において、AIシステムに生じ得るリスク分析が技術その他の制約により十分に実施できない場合には、開発型契約単体でリスク調整を行うのではなく、その後当事者間で締結される契約で段階的に調整をすることで、より実態に即したリスク分配が可能となる場合も想定される。

【権利帰属/利用条件】

- アウトプットの権利帰属及び利用条件は、ユーザとベンダの利害が先鋭的に対立しやすい事項である。開発型契約では、開発により創出された成果に関する知的財産をフォアグラウンドIP、開発と関係なく各当事者が有する知的財産をバックグラウンドIPと位置づけた上で、前者に関する権利帰属や利用条件が契約上議論されることが少なくない。もっとも、当事者間において、議論の対象のアウトプットの具体的な範囲が十分に認識されないまま開発が進み、その権利帰属や利用条件を決定する段階に至って、アウトプットがフォアグラウンドIPを構成するのか、それとも、ベンダのバックグラウンドIPを構成するのかが争点になることも想定される。
- 特に、**【類型2：カスタマイズ型】**において開発型契約が締結される場合、アウトプットがベンダ提供のAIシステム又はAIサービスと組み合わせて利用されることから、当事者でアウトプットがフォアグラウンドIP又はバックグラウンドIPに該当するのかを明確に整理せずに開発が進む場合がある。AIシステムに関する開発は長期間にわたり継続することもあり、開発が進むにつれてアウトプットの具体的な範囲が不明確になることがあるため、開発初期の段階で当事者の認識を擦り合わせることが重要である。

4.4 個人情報保護法に関する留意点

AI関連サービス[13]の利用に伴い、ユーザからベンダに対し提供するインプットに個人データが含まれる場合[14]、個人情報保護法の第三者提供規制（個情法27条）の遵守が必要になる。また、AI関連サービスの提供には海外ベンダが関与している事例が多く見られるところ、上記場合においてベンダが外国に所在するときには、さらに越境移転規制（個情法28条）の遵守が必要となるため、注意を要する。

契約との関係では特に以下の各点の検討が重要である[15、16]。なお、以下では、「ユーザ」がAIサービスの利用に伴って個人データを含むインプットを提供する立場にあり、「ベンダ」がインプットの提供を受ける立場にある。

4.4.1 国内の第三者への個人データの提供に該当する場合

個人情報取扱事業者たるユーザが、AI関連サービス利用のために個人データを含むインプットを提供する場面において、インプットが個人データの第三者提供（個情法27条1項）に当たる場合[17]、ユーザは原則としてあらかじめ本人の同意を取得し（個情法27条1項）、かつ、第三者提供に係る記録を作成等する義務（個情法29条）を負う。

他方、例えば、ベンダに対する個人データの「提供」が、利用者の利用目的の達成に必要な範囲内において個人データの取扱いを「委託」すること（個情法27条5項1号）に伴って行われる場合には、当該「提供」についてあらかじめ本人の同意を得る必要はない。

13. 上記2.1のとおり、AI関連サービスは、システム提供型とサービス提供型の両方を含んでいることには留意が必要である。

14. 「個人データ」とは、「個人情報」（個情法2条1項）のうち「個人情報データベース等」を構成するものをいう（個情法16条3項）。この「個人情報データベース等」とは、特定の個人情報をコンピュータを用いて検索することができるように体系的に構成した、個人情報を含む情報の集合物をいう。また、コンピュータを用いていない場合であっても、紙面で処理した個人情報を一定の規則（例えば、五十音順等）に従って整理・分類し、特定の個人情報を容易に検索することができるよう、目次、索引、符号等を付し、他人によっても容易に検索可能な状態に置いているものも該当する（個情法16条1項、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（通則編）」2-4）。

15. チェックリストでは、あくまでも契約との関係で重要と思われる規律を記載しているにすぎず、個人情報保護法上遵守が必要な規律の全てを定めているものではないため、留意されたい。

16. なお、ユーザは、あらかじめ本人の同意を得ないで、特定された利用目的の達成に必要な範囲を超えて、個人情報を取扱ってはならない（個情法18条）。そのため、ユーザは、インプットに含まれる個人情報が個人データには該当しない場合であっても、インプットに個人情報を含めることが利用目的の達成に必要な範囲内か否かに留意する必要がある。

17. 契約条項によってベンダがサーバに保存された個人データを取扱わない旨が定められており、適切にアクセス制御を行っている場合等、ベンダが当該個人データを取扱わないこととなっている場合には、個人データの提供がないとされている（個人情報保護委員会Q&A Q7-53）。なお、この場合でも、ユーザは、自ら果たすべき安全管理措置の一環として、適切な安全管理措置を講じる必要がある（個人情報保護委員会Q&A Q7-54）。

- このときベンダ（委託先）は、委託された業務以外に、委託に伴ってユーザ（委託元）から提供された個人データを取扱うことはできない。当該業務以外に当該個人データを取扱う事例として、例えば次のような事例が考えられるため、注意を要する。
  - ベンダが、ユーザの利用目的の達成に必要な範囲を超えて、委託の内容と関係のない自社の活動のために個人データを取り扱うとき。
  - ベンダが、委託に伴ってユーザから提供された個人データを、当該ベンダが独自に取得した個人データ又は個人関連情報と本人ごとに突合するとき[18]。
- ユーザ（委託元）には、必要かつ適切な安全管理措置の一環として、委託先の監督義務（個情法25条）が課せられ、（1）適切な委託先の選定、（2）委託契約の締結及び（3）委託先における個人データの取扱状況の把握の観点から、必要かつ適切な措置を講じなければならない。
  - （2）委託契約の締結に関し、委託契約には、当該個人データの取扱いに関する、必要かつ適切な安全管理措置として、ユーザ・ベンダ双方が同意した内容とともに、ベンダにおける委託された個人データの取扱状況をユーザが合理的に把握することを盛り込むことが望ましい[19]。
  - （3）ベンダにおける個人データの取扱状況の把握に当たっては、取扱いを委託する個人データの内容や規模に応じて適切な方法を講じれば足りる[20]。ベンダの監督については、取扱いを委託する個人データの内容を踏まえ、個人データが漏えい等をした場合に本人が被る権利利益の侵害の大きさを考慮し、委託する事業の規模及び性質、個人データの取扱状況（取扱う個人データの性質及び量を含む。）等に起因するリスクに応じて行うべきものと考えられる[21]。したがって、具体的にどのような内容の監督義務を講ずべきかは個々の事案により異なるが、例えば、ベンダの約款等を吟味した結果、当該約款等を遵守することにより当該個人データの安全管理が図られると判断される場合には、それをもって監督義務の履行として十分と考えられるケースもあり得る。

個人情報取扱事業者たるユーザが、あらかじめ本人の同意を得ることなく生成AIサービスに個人データを含むプロンプトを入力し、サービス提供者が当該個人データを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う場合、当該ユーザは個人情報保護法の規定に違反することとなる可能性がある[22]。

18. 個人情報保護委員会Q&A Q7-41
19. 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（通則編）」3-4-4（2）
20. 個人情報保護委員会Q&A Q5-9
21. 個人情報保護委員会Q&A Q5-11
22. 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」（1）②

4.4.2 外国[23]にある第三者への個人データの提供に該当する場合

インプットの提供先であるベンダが「外国にある第三者」に該当するかは、外国の法令に準拠して設立され外国に住所を有する外国法人であること等が考慮要素となるが、個別具体的な検討を要する[24]。提供したインプットが保存されるサーバの所在地は判断基準とはならないため、注意が必要である[25]。

ベンダが外国にある第三者である場合、次に定める場合を除き、あらかじめ「外国にある第三者への個人データの提供を認める」旨の本人の同意を得る必要がある。当該同意の取得に際しては、その外国の名称、その外国の個人情報の保護に関する制度、及びベンダが講じる個人情報の保護のための措置に関する情報[26]を本人に提供する必要がある。

- その外国が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法施行規則で定める外国である場合[27]
- 個人情報取扱事業者が講ずべき措置に相当する措置を継続的に講ずるために必要な体制として個人情報保護法施行規則で定める基準に適合する体制（**基準適合体制**）（下記参照）を整備している場合
- 個人情報保護法27条1項各号に定める場合

基準適合体制の整備としては、以下のいずれかの要件を充足する必要がある。なお、ユーザは、個人情報保護法施行規則で定めるところにより、ベンダによる相当措置の継続的な実施を確保するために必要な措置を講ずる[28]とともに、本人に対し、その求めに応じて当該必要な措置に関する情報を提供する義務[29]を負う[30]。

23. 本邦の域外にある国又は地域をいう。

24. 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）」（外国第三者提供GL）2-2。ベンダが外国の法令に準拠して設立され外国に住所を有する外国法人であっても、例えば、日本国内に事務所を設置している場合、又は、日本国内で事業活動を行っている場合等、日本国内で「個人情報データベース等」を事業の用に供していると認められるときは、当該ベンダは、「外国にある第三者」には該当しない。

25. 例えば、個人情報取扱事業者であるユーザが自ら外国に設置し、自ら管理・運営するサーバに個人データを保存することは、外国にある第三者への提供には該当しない（個人情報保護委員会Q&A Q12-3）。また、ベンダがA国に所在しているものの、B国にサーバを設置しており、提供した個人データが当該サーバに保存される場合は、サーバ所在地であるB国ではなく、A国にある第三者への越境移転となる（個人情報保護委員会Q&A Q12-11）。

26. 個情法28条2項、個情規則17条2項、外国第三者提供GL 5-2

27. チェックリスト公表日現在、EEA加盟国及び英国がこれに該当する。

28. 個情規則18条1項、外国第三者提供GL 6-1

29. 個情規則18条3項、外国第三者提供GL 6-2

30. 個情法28条3項。外国にあるベンダと契約する際には、日本の個人情報保護法の規律を十分に把握しているとは限らないため、必要に応じて規律の内容を十分に説明し、対応を求めることが必要になる場合もある。

- ベンダとの間の契約等、「適切かつ合理的な方法」により、下表に記載された個人情報保護法第4章第2節の規定の趣旨に沿った措置（相当措置）の実施が確保されていること[31]

第17条	利用目的の特定	**第27条**	第三者提供の制限
第18条	利用目的による制限	**第28条**	外国にある第三者への提供の制限
第19条	不適正な利用の禁止	**第32条**	保有個人データに関する事項の公表等
第20条	適正な取得	**第33条**	開示
第21条	取得に際しての利用目的の通知等	**第34条**	訂正等
第22条	データ内容の正確性の確保等	**第35条**	利用停止等
第23条	安全管理措置	**第36条**	理由の説明
第24条	従業者の監督	**第37条**	開示等の請求等に応じる手続
第25条	委託先の監督	**第38条**	手数料
第26条	漏えい等の報告等	**第40条**	個人情報取扱事業者による苦情の処理

- ベンダがAPECのCBPRシステムの認証を取得している企業（以下「**CBPR認証企業**」という。）である等、個人情報の取扱いに係る国際的な枠組みに基づく認定を受けていること[32]

31. 個情規則16条1号。契約等において、表の全ての事項を記載しなければならないものではなく、措置の実施が必要な範囲で確保されていれば足りる（外国第三者提供GL 4-1及び4-2）。なお、ユーザがCBPR認証企業であり、ベンダが当該ユーザに代わって個人情報を取扱う者である場合には、当該ユーザがCBPRの認証の取得要件を充たすことも、「適切かつ合理的な方法」の一つとなり得る（外国第三者提供GL 4-1）。

32. 個情規則16条2号、外国第三者提供GL 4-3。

4.4.3 個人情報保護法27条及び28条の適用関係の整理

個人情報保護法27条及び28条の適用関係[33]は、下表のとおりである。インプットの提供[34]を受けるベンダが日本にある第三者である場合には、同法27条の第三者提供規制が主な論点となるが、外国にある第三者である場合には、上記4.4.2に述べた同法28条に基づく提供根拠を整理した上で、同条に基づく同意を得た場合を除き、さらに同法27条に基づく規律を遵守することが必要となる。

<table>
<tr><th></th><th>個人情報保護法28条に基づく提供根拠</th><th>個人情報保護法27条に基づく規律</th></tr>
<tr><td rowspan="3">外国にある第三者</td><td>外国にある第三者への提供を認める旨の本人の同意を取得すること[35]

※同意の取得に際しては、その外国の名称、その外国の個人情報の保護に関する制度やベンダが講じる個人情報の保護のための措置に関する情報を本人に提供する必要がある</td><td>―

（個人情報保護法28条に基づく同意を得た場合には、同法27条の規定は適用されない[36]）</td></tr>
<tr><td>ベンダが基準適合体制を整備していること

※ユーザは、個情規則で定めるところにより、ベンダによる相当措置の継続的な実施を確保するために必要な措置を講ずるとともに、本人の求めに応じて当該必要な措置に関する情報を当該本人に提供する必要がある</td><td rowspan="3">第三者への提供に当たる場合は、そのような提供を認める旨の本人の同意を取得する必要がある

※実務上活用されることが多い第三者提供の例外として委託構成があり、インプットの提供が、ユーザの利用目的の達成に必要な範囲内において個人データの取扱いの「委託」[37]に伴って行われる場合には、「第三者」への提供には当たらず、あらかじめ本人の同意を得る必要はない（委託構成に関する留意事項については上記4.4.1参照）</td></tr>
<tr><td>ベンダが、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情規則で定める外国であること（チェックリスト公表日現在、EEA加盟国及び英国がこれに該当する）</td></tr>
<tr><td>日本にある第三者</td><td></td></tr>
</table>

また、上記の適用関係に関し、検討の主なポイント及び流れを図式化すると、図9のとおりとなる。

33. 個情法27条1項各号に定める場合には、本人の同意なく個人データを第三者（外国にある第三者を含む）に提供することができる。以下の説明では、個情法27条1項各号に該当しない場合の取扱いを説明する。

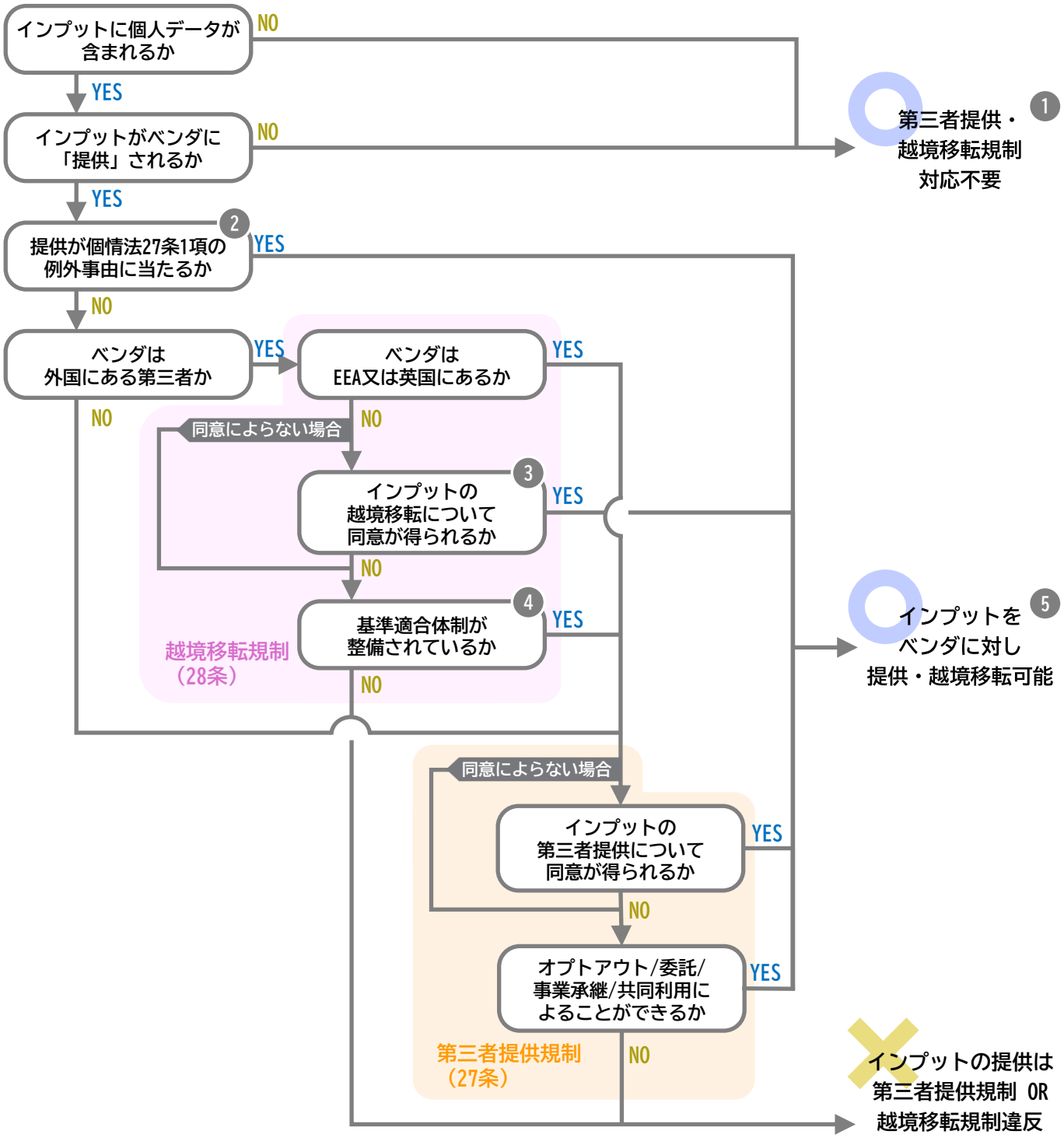
34. 上記注17のとおり、契約条項によってベンダがサーバに保存された個人データを取扱わない旨が定められており、適切にアクセス制御を行っている場合等、ベンダが当該個人データを取扱わないこととなっている場合には、個人データの提供がないとされている（個人情報保護委員会Q&A Q7-53）。なお、この場合でも、ユーザは、自ら果たすべき安全管理措置の一環として適切な安全管理措置を講じる必要がある（個人情報保護委員会Q&A Q7-54）。また、外国にあるベンダの提供するクラウドサービスを利用する場合は、ベンダに対する個人データの提供がない場合であっても、ユーザは、外国において個人データを取扱うこととなるため、当該外国の個人情報の保護に関する制度等を把握した上で、安全管理措置を講じる必要がある。具体的には、原則として、ベンダが所在する外国の名称及び個人データが保存されるサーバが所在する外国の名称を明らかにし、当該外国の制度等を把握した上で講じた措置の内容を本人の知り得る状態に置く必要がある（詳細は、個人情報保護委員会Q&A Q10-25参照）。

35. 本人の同意に基づいて越境移転を行う場合、第三者提供の例外としての委託等（個情法27条5項）に相当する例外規定が存在しないため、注意を要する。

36. 個情法28条1項第2文。

37. 個情法27条5項1号。

図9　個人情報保護法27条及び28条の適用関係の整理



注記

1. ベンダに対する個人データの提供がない場合であっても、ユーザは、自ら果たすべき安全管理措置の一環として、適切な安全管理措置を講じる必要がある。また、外国において個人データを取扱うこととなる場合、当該外国の個人情報の保護に関する制度等を把握した上で、安全管理措置を講じる必要がある。なお、インプットに含まれる個人情報が個人データには該当しない場合であっても、利用目的規制等は別途問題となるため注意が必要である
2. 当該例外事由は個情法27条及び28条に共通して適用されるところ、作図の便宜上、各規制の枠外に位置づけている
3. 同意の取得に際しては、その外国の名称、その外国の個人情報の保護に関する制度及びベンダが講じる個人情報の保護のための措置に関する情報を本人に提供する必要がある
4. ユーザは、個人情報保護委員会規則で定めるところにより、ベンダによる相当措置の継続的な実施を確保するために必要な措置を講ずるとともに、本人の求めに応じて当該必要な措置に関する情報を当該本人に提供する必要がある
5. 個情法28条のルートを取る場合には越境移転が可能であり、同法27条のルートだけを取る場合には提供が可能である

4.5 セキュリティに関する留意点

上記4.2で述べたとおり、ユーザが利用しようとするAI関連サービスの形態に応じて、システムの構造やセキュリティ水準に関し一定程度慎重に検討を行うべき場合がある。

データセキュリティに関する契約条項としては、チェックリスト（A-3-3）や（A-3-4）のとおり、インプットを処理するアプリケーションを含むAIシステム全体（**対象システム**[38]）のセキュリティ水準、監査・情報提供義務、ログ保存義務等の条項が主な検討対象となる。以下、ユーザ側の契約担当者が、場合によっては社内の技術担当者等とも協業しながら、関連する契約条項を検討する際に有益と考えられる具体的な着眼点を示す。なお、AIサービスが商用データセンタあるいはパブリッククラウド等の第三者の環境下で運用される場合、AIサービスの扱うデータに当該第三者自身がアクセスすることが技術的に不可能な状況が確保されているかは、契約条件だけでなく、実際のセキュリティレベルにも大きく依存するため、契約締結の際にはこのような観点からの情報収集及び検討も重要である。

38. なお、対象システムが下位システムに依存している場合（同一ベンダ内だけでなく、第三者の下位のクラウド等の基盤システムに依存している場合を含む） や他のシステムを水平的に呼び出している場合 （例えば、AI関連サービスが外部のID認証サービスを呼び出している場合等。当該外部ID認証サービスがセキュリティ侵害を受けると、攻撃者は当該AI関連サービスの情報にアクセスできてしまう）、対象システムのセキュリティ強度は各依存先システムのセキュリティ強度のうち最も弱いものに依存することから、物理 （ハードウェア） 的セキュリティに達するまでの全てのシステムにおけるセキュリティが論点となり得る。

4.5.1 対象システムのセキュリティ水準

ユーザは必要に応じて、利用しようとするAIサービスがユーザの要求する機密水準に適合したセキュリティ水準を有しているかを確認し、重要なセキュリティ要件が契約内容に反映されているかを検討する必要がある。ただし、対象システムのソースコードや設計の詳細は、ベンダの企業秘密に該当するとして、開示されない場合も少なくない。その場合、どのような資料を参照すべきかについて必ずしも定まった手法は存在しないが、例えば以下のような資料は重要な参考資料となり得る。ベンダに任意の資料開示を求めることや、必要に応じて契約上もこれらの資料の継続的な開示を求めることも考えられる。

【対象システムのアーキテクチャに関する資料】

- 対象システムのセキュリティ強度を外部的に推測するために、設計・実装の思想や実際の構造を示す多様な資料の確認が重要である。ベンダが広報目的で作成した資料だけでは、実際のセキュリティレベルを把握することは難しい。そこで、ベンダ内の技術者あるいは信頼できる執筆者[39]によるアーキテクチャ全体図、書籍、技術記事、論文、ホワイトペーパー、講演資料等、幅広いものを確認する方法が有用である。その際、文書相互の記述の正確性・一貫性等を元に対象システムのセキュリティ水準を一定程度正確に確認でき[40]、確認する資料の記述者や内容の多様性を確保できるならば、個々の記載の粒度は必ずしも詳細である必要はなくなる。

【ソフトウェア部品構成表：Software Bill of Materials （SBOM）】

- 対象システムに含まれる全てのソフトウェアコンポーネントや依存関係を一覧化した文書としてはSBOMが有用であり、脆弱性の特定や管理を容易にする効果が期待される[41]。

39. 多数のユーザや読者から内容のレビューを受けることを前提として、著者が自己の名において見解を発表しているものが望ましい。

40. 例えば、Microsoftの技術者達が外部著者に協力し、自社のクラウド基盤を構成するソフトウェアの構造を解説し、独自に実装しているセキュリティ対策を解説している書籍がある[1]。また、Googleの技術者が、自社クラウド基盤ソフトウェアの構造を示し、不要なプログラムを極力排除することによりアタックサーフェスの最小化措置を講じていることを説明する同社ウェブサイトのような例も存在する[2]。このような公表物も、システムないしそれを構成する要素技術について、設計・実装の思想や実際の構造を示した資料に当たる。
[1] Pavel Yosifovich他（著）、山内 和朗（訳）「インサイドWindows第7版」（2018年、日経BP）他「インサイドWindows」シリーズ
[2] Andy Honig他「7 ways we harden our KVM hypervisor at Google Cloud: security in plaintext」（2017年）https://cloud.google.com/blog/products/gcp/7-ways-we-harden-our-kvm-hypervisor-at-google-cloud-security-in-plaintext?hl=en （2024年12月4日閲覧）

41. SBOMによる脆弱性管理プロセス等の観点でユーザの参考になる文書として、経済産業省「ソフトウェア管理に向けたSBOM（Software Bill of Materials）の導入に関する手引ver2.0」（2024年8月29日）参照。なお、個々のコンポーネントに脆弱性が認められたとしても、それが対象システム全体のセキュリティリスクに繋がるか否かは、当該コンポーネントの機能や役割次第であるため、対象システムのアーキテクチャに関する資料とともに分析し、必要に応じてベンダに質問をすることが望ましい。

【脆弱性情報】

- 脆弱性の発見・修正履歴や脆弱性ニュース等において、対象システムのプログラムの規模や複雑さに応じ[42]、脆弱性が第三者によって発見されベンダによって修正された事例の蓄積があれば、多角的な第三者による客観的な脆弱性の調査が行なわれ、継続的に発見・対策されていると評価できるため、セキュリティ強度を推認する一要素となる。

4.5.2 監査条項等

可能な場合には、監査条項を設けることも有効である。例えば、第三者である委託事業者の内部監査部門による監査等の条項や、国際的なセキュリティの第三者認証（ISO/IEC27001等）の取得を条件とする方法等が考えられる。

4.5.3 ログの保存

サイバー攻撃への対応や内部不正防止の観点から、ユーザによるアプリケーション利用のログだけでなく、AIサービス及びその基盤部分に対する管理者・開発者権限を含む認証ログ、アクセスログ、操作ログ等の各種ログを保存するようベンダに求めることも考えられる。

4.6 規約改定に関する留意点

上記で取り上げた利用型契約のうち、ベンダが利用規約に基づいてサービスを提供しているケースでは、利用規約が定期的に変更され得るため、変更状況を随時確認すべきことに留意が必要である。利用規約の変更条件や手続等については、利用規約に定められた規約変更に関する条項や、利用規約が選択する準拠法がこれを規律することとなる。特にベンダが海外に所在する場合には、海外法が準拠法として選択されることが多いため、ユーザは、必要に応じて選択された準拠法における規約変更のルールを確認することが望ましい。

日本においては、一定の条件を満たす利用規約に関する民法上のルールが存在する。利用規約が民法上の定型約款（民法548条の2）に該当する場合[43]、ベンダは、その変更内容がユーザの一般の利益に適合しない場合であっても、①利用規約を変更する旨、②変更後の利用規約の内容、及び③効力発生時期を、その効力発生時期が到来する前に、インターネットの利用やその他の適切な方法により周知する場合には、その変更が合理的なものである限り、ユーザの個別の同意を必要とせずに契約の内容を変更することができる（民法548条の4）。しかし、利用規約の変更がウェブサイト等で周知されるに留まる場合、ユーザがそのような変更を把握しないままAI関連サービスを利用し、その結果、契約違反相当行為を行う、又は不測のインプット

42. 脆弱性はプログラム上のコーディングミス又はロジックの誤りで生まれるが、規模や複雑さに応じて誤りは増加し、これを避けることは不可能である。したがって、大規模なプログラムには不可避的に脆弱性が多く存在することとなり、規模が巨大であるにもかかわらず脆弱性がほとんど報告されていないようなサービスは、脆弱性の調査や対処が行なわれないまま残存している懸念が残る。

43. チェックリストはAI利用に関する契約上の留意点を取りまとめることを目的としているため、どのような利用規約が定型約款に該当するか等の民法の解釈適用に関する解説は、各種文献に譲る。

利用が発生する等の事態が想定される。これらの事態を避けるため、ユーザは利用規約の内容及び変更状況を随時確認するための体制を整備することが望ましい。

また、上記**【類型2：カスタマイズ型】**のように、汎用的AIサービスをカスタマイズして提供するような場面では、汎用的AIサービスの利用規約を基にして、さらにカスタマイズされたサービスの利用規約が作成される。カスタマイズサービスを提供するベンダは、その基となる汎用的AIサービスの利用規約の変更に応じ、これと連動する形でカスタマイズサービスの利用規約を変更する必要が生じる場合がある。そのため、上記のチェック体制の整備がより一層求められることから、必要に応じて、関連する規約の更新をチェックする担当者や部署等を検討することも一案である。

経済産業省

経済産業省　商務情報政策局　情報経済課

経済産業省　商務情報政策局　情報産業課　情報処理基盤産業室

経済産業省　製造産業局　総務課　DXチーム

AI利活用に伴う契約時の留意事項検討会

松下　外（主査）

生貝　直人

齊藤　友紀

殿村　桂司

西田　亮正

登　　大遊