生成ＡＩの適切な利活用等に向けた知的財産の保護及び透明性に関するプリンシプル・コード（仮称）（案）に対する提出意見案

2026 年 1 月 26 日　新経済連盟

1．「総論」に対する意見

（1）基本的な考え方（目的）

- 本プリンシプル・コード案には、「人工知能関連技術の研究開発及び活用の推進に関する法律」（令和 7 年法律第 53 号）の趣旨を踏まえつつ、という記載があるが、同法のどの条文に基づくものなのか法的な位置づけを明確にすべき。
- EU AI Act の取組やコーポレートガバナンス分野におけるスチュアードシップコード等の取組に言及されているが、上場会社の多くは、投資家やユーザーをはじめとするステークホルダーに対し、コーポレートガバナンス報告書や有価証券報告書等を通じて、透明性の高い情報開示を継続的に実践している。仮に本プリンシプル・コードに基づく開示を実施する場合においても、例えば、独自の報告形式を新設するのではなく、これら既存の開示枠組みへの記載をもって代替可能とすることを要望する。情報発信媒体の集約化をすることで、事業者の事務負担を軽減するだけでなく、情報の視認性や比較可能性を高め、権利者、サービスのユーザーや投資家にとってもより生成 AI に関する情報にアクセス容易な環境及び有益な情報提供を行うことができ得る選択肢もあると考える。
- １頁「１．（１）基本的な考え方」及び２頁「１．（３）この文書が採用する手法」において、本プリンシプル・コード案に「コンプライ・オア・エクスプレイン」の手法を導入する旨の記載があるが、各原則を実施しない理由（エクスプレイン）の具体的内容や基準が不透明である。コンプライの事例及びエクスプレインの事例について、それぞれ好事例集を整理し、政府当局として開示することを検討されたい。なお、特に、取引先との守秘義務や競争力の源泉である営業秘密を保持する必要がある場合、詳細な開示は困難となるケースもあることから、その点に配慮し、好事例集を開示すべきと考える。
- 現在、資本市場では AI ガバナンスへの要請が急速に具体化しており、米グラス・ルイス社の『Proxy Paper Guidelines』での言及に見られるように、これが評価基準の一部に組み込まれつつある。このような状況下では、本プリンシプル・コードが法的拘束力を持たない指針であっても、実態として「非対応＝不誠実」という評価を招き、企業のレピュテーションに多大な影響を及ぼす（事実上の強制力を持つ）懸念がある。こうした懸念を払拭するため、守秘義務等の正当な理由で「エクスプレイン」を選択した企業に対し、不当な社会的評価が生じないような配慮や周知を行う予定はあるのか。

（2）この文書の適用を受ける対象

- 本プリンシプル・コード案における「生成 AI 提供者」の定義は非常に広範である。また、生成 AI 開発者と、API 等を通じて他社である生成 AI 開発者が開発したモデルを利用する生成 AI 提供者を一律に扱うことは、実効性を欠くだけでなく事業者の予見可能性を損なうおそれがある。特に、他社モデルを利用してサービス提供を行う生成 AI 提供者は、モデル開発者が

非開示としている学習データの詳細や内部構造を物理的に把握することが不可能である。自社で制御・把握不可能な事項についてまで一律の開示・説明義務を負わされることは、事業者にとって過度な実務負担となるだけでなく、把握不能を理由とした不当な社会的評価を受けるリスクを生じさせる。

- 本プリンシプル・コード案では、「生成ＡＩ開発者」及び「生成ＡＩ提供者」（以下これらを総称して「生成ＡＩ事業者」という。）に適用されるものとするとあるが、対象となる生成 AI システムに特段の限定がないため、チャットボットや推論・提案型 AI も「生成 AI」に含まれるのか不明確であり、現状では全ての生成 AI システムを組み込んだサービスが対象になりかねない。また、不正取引検知やコンテンツ・モデレーション等での生成 AI 利用も対象となれば、情報開示を行うこと自体にシステムハックやセキュリティ上の懸念が生じる。
- EU AI Act が、学習データに関する一般向けの透明性確保や著作権対応の直接的な義務対象を原則として「汎用 AI モデル（GPAI）のプロバイダー」に限定しているのに対し、本文書は、「生成 AI 提供者」までも対象としており、適用を受ける対象範囲が著しく広範である。「生成 AI 提供者」は、基盤モデルの学習データセットや詳細なアーキテクチャ等を関知し得ない立場にある。それにもかかわらず、開発者と同等の説明責任や個別の照会対応（原則 2 等）を求めることは、事業者に対し過度な負担を強いるものである。したがって、「生成 AI 提供者」については、学習データやモデルの構造に関する透明性確保・権利侵害対応の対象から除外すべきである。
- 本プリンシプル・コードの策定の趣旨が、日本のコンテンツの産業や個人クリエイターの知的財産権等の保護にあるのであれば、「利用者が権利侵害リスクのあるコンテンツ生成を行うことができる生成 AI システム」にその範囲を限定すべき。また、そのような生成ＡＩシステムに範囲を限定した上で、ＡＩ提供企業の主要なサービスのみを開示の対象とするなど、対象範囲を限定すべきであると考える。
- 広告キャンペーン等の期間限定サービス（例：ユーザーが自分の顔写真をアップして AI 画像を生成する特設サイトを公開する、など）が「生成 AI 提供者」に該当するか、定義の明確化を求める。基盤モデル開発者とサービス実装者の開示義務を切り分け、短期間の提供者に継続的な公表や年 1 回の見直しを強いる過大な負担は避けるべき。特にログ保存は、キャンペーン終了後のデータ保持リスクを考慮し、柔軟な運用を要望する。
- また、企画書検索など社内データを用いた業務効率化ツール（RAG 等）が「生成 AI 提供者」の対象外とされている点を強く支持する。公衆向けではない社内・グループ内限定のシステムについては、公表義務等の対象外であることを確定版でも明記すべき。過度な事務負担で企業の DX を阻害しないことを要望する。

（4）この文書の受入れ状況の可視化

- 本プリンシプル・コード案では毎年の更新公表が期待されているが、公表すべき情報の粒度が過度に詳細である場合、以下のような重大な経営リスクが生じる懸念がある。

1．機密保持及び競争力の維持上のリスク：

具体的な侵害対策やアルゴリズム、内部の意思決定プロセスが詳細に公表されることで、

改善ポイントや開発サイクルが競合他社に推測され、技術的な優位性が損なわれるおそれがある。

2．セキュリティ上のリスク：
侵害対策の詳細な開示は、悪意のある第三者に対策を回避するヒントを与えることになりかねず、安全な利用環境の確保という本プリンシプル・コードの目的に逆行する可能性がある。

したがって、情報の公表にあたっては、形式的な詳細さを求めるのではなく、「基本的な考え方」で要望したとおり、既存のコーポレートガバナンス報告書や有価証券報告書による代替可能性を認めるなど、柔軟な運用を担保すべき。

- また、「開示内容の審査は行わない」とされている点（3 頁上から 5 - 6 行目）に関連し、公表する情報の具体的な粒度については、事業者が経営リスク（競争力やセキュリティ）を考慮して行う「合理的な判断」が最大限に尊重され、それに異議を唱えないという趣旨と理解。実務上の過度な負担を抑えつつ持続可能な透明性を確保するため、事業者の主体的な判断に委ねる運用であることを改めて確認したい。また、そのプロセスや、公表方法が適切なものとなるように、デジタル庁などと連携をいただき、届出や更新手続きにあたっては e-Gov や G ビズポータル、公表に当たっては G ビズインフォとの連携を図ること等を期待する。
- 現在コード案に記載されている届出・公表等の運用は、企業だけでなく内閣府知財戦略推進事務局における運用・管理等にもコストがかかるものであると想定されるため、広島 AI プロセス（HAIP）等の国際的な枠組みに委ねるべきであると考える。また、原則 1 における開示情報を常に最新の状態に保つことは、変化の激しい AI 技術開発の状況を鑑みると現実的ではなく、日本国内でサービス展開する事業者のみにそのような負担を課すことは、国際的なイコールフッティングの観点でも不適切な規制となりえる。

2．「この文書が示す原則及び例外」に対する意見

【原則 1】

- 生成 AI 提供者の多くは、生成 AI 開発者が構築したモデルを外部から利用する形態をとっており、生成 AI 開発者が非開示としている学習データの詳細等を把握することは物理的に不可能。生成 AI 開発者の開示事項をそのまま重複して開示することは実務的な意義が乏しく、また、生成 AI 開発者が開示していない事項を生成 AI 提供者に求めることは予見可能性を著しく損なう。したがって、生成 AI 提供者においては、生成 AI 開発者の情報提供に基づく開示を原則とした上で、自社における「モデル選定の方針」や「ガバナンス体制」など、生成 AI 提供者として管理・制御可能な範囲に開示項目を限定すること、及び生成 AI 提供者においては、生成 AI 開発者の開示内容を参照し開示を行うことを許容することにつき、本プリンシプル・コード内で明示されたい。
- 特に AI 提供者についてみた場合、開発されたモデルを自社サービスに組み込む「生成 AI 提供者」に対し、開発者レベルの詳細な情報（データの収集期間やクローラの識別子等）の開示を求めるのは過剰。 1 つのサービスに複数の AI 機能を搭載する場合、すべての機能に対してこ

れら多岐にわたる項目の見直し・更新を毎年行うことは、開発スピードを著しく停滞させ、イノベーションを阻害する「制度的障壁」となる。

- 開示対象は知的財産の保護・透明性の目的に直接関係する事項に限定し、営業秘密、セキュリティ上の懸念、契約上の守秘義務、個人情報保護等に抵触し得る情報については、非開示を明確に許容すべきである。法務・税務・人事等の高度専門職領域を扱うAIサービスでは、顧客の機密性が高い情報（訴訟戦略、契約交渉方針、証拠関係、納税額、採用選考情報、その他個人情報等）が入力・出力に含まれ得ることに加え、サービスの安全性確保のため、攻撃面を増大させ得る情報（システム構成や運用の詳細、過度に踏み込んだ内部仕様等）は厳格に管理する必要がある。加えて、RAG（検索拡張生成）技術等を用い、利用者が保有する極めて機密性の高い内部文書（契約書、未公開特許、人事データ等）を回答生成の根拠とすることが一般的である。原則1の開示対象が、こうした「利用者固有の参照データ」や「プロンプトエンジニアリングのノウハウ」にまで及ぶと解釈される余地が残ると、営業秘密の毀損やセキュリティリスクの増大を招き、結果としてサービス提供の萎縮（機能制限、提供回避、国内提供停止等）につながりかねない。このような領域において「すべての者が閲覧可能」な形で広範な事項の公表を求める設計は過剰な実質的規制であり、利活用促進という政策目的の観点からも、公開前提の整理と、目的適合的な範囲への限定が必要である。

（1）透明性確保のための措置、について

- 本案で求められているアーキテクチャやトレーニングプロセスの詳細な開示は 、情報の粒度が細かすぎる懸念がある。これらを開示したとしても、その技術的内容を正確に理解できる利用者は極めて限定的であり 、実効性に疑問が残る。また、知的財産権侵害を防止するフィルタリング等の技術的措置を講ずることとされているが 、生成AIの性質上、全ての侵害を完全に防ぐことは技術的に極めて困難。事業者に対し、一律に実効性が不明確な措置を求めることは、開発現場の実情に即しておらず現実的ではない。形式的な情報開示や、実現困難な技術的義務を課すのではなく、より本質的で実効性のある開示基準への整理を検討すべき。
- 「ア　使用モデル関係」について、SaaS事業の現場においては、顧客への価値提供を最適化するため、一つのサービス内で複数の生成AIモデルを組み合わせたり（マルチモデル）、機能改善のために短期間でモデルを入れ替えたりすることが一般的。本プリンシプル・コード案において示された「すべてのモデル」の概要開示を一律に求めることは、以下の観点から実務上の合理的範囲を超え、事業活動に支障をきたす懸念があることから、使用モデルの内容や数などを限定するなど、開示内容を限定していただきたい。また、現時点で想定している、使用モデルに関する開示内容の粒度、範囲又は内容（例：使用しているモデルのすべてか／サービスごとか／利用数の上位のみか等）を明らかにすべき。
- 「イ　学習データ関係」に掲げられた特定の技術情報は、各事業者が多大な投資と試行錯誤を通じて構築した、競争優位性の根幹に関わる機密情報である。これらをサービス単位で開示させることは、以下のリスクを招く懸念があるため、開示項目からの削除、あるいは開示を必須としない運用の徹底を求める。

  1．技術的優位性の流出と模倣の誘発：

独自のアーキテクチャ、トレーニングプロセス及びプロンプトエンジニアリング等のノウハウは、事業者の技術的な独自性を担保するものである。これらが開示対象に含まれる場合、他社による容易な模倣を許し、わが国の AI 産業における健全な競争や国際競争力の低下を招くおそれがある。こうした情報をあえて開示対象に含めることは、わが国の AI 産業の競争力強化という目的に照らして矛盾する。

2．セキュリティ及び安全上のリスク：
特に「クローラの識別子」や「アーキテクチャの詳細」の開示は、システムの脆弱性を探る攻撃や不当なアクセス、あるいは防御策の回避を試みる第三者に端緒を与えることになりかねない。安全な AI 利用環境の確保という本プリンシプル・コードの目的に照らせば、これらセキュリティに直結する情報は非開示、あるいは削除されるべき。

3．技術革新への制約：
独自のデータ収集手法やクローリングの改善は技術進展に伴い動的に行われるところ、詳細なプロセスの公表は、迅速な技術革新を阻害する要因となる。開発現場に過度な事務的制約を課し、開発スピードを低下させる懸念に対し、どのような対策や配慮を検討されているのかを明らかにすべき。

- 利用者にとって有益な透明性とは、機密性の高い技術詳細の開示ではなく、「生成 AI モデルやそれを活用したサービスが適切に管理・運用されているか」という AI ガバナンスの透明性にあると考える。したがって、技術仕様の詳細公表を求めるのではなく、意思決定プロセスやモニタリング体制といった運用面の開示に重点を置いた制度設計を要望する。
- 「アーキテクチャ・設計仕様」「モデルのトレーニングプロセスの内容」「クローラの識別子」については、削除すべきではないか。これらは生成 AI 提供者にとって他社との競争優位性を保つ上で非常に重要なコア技術であり、サービス単位で開示することは、他社による模倣を容易にし、適性な競争を害するおそれがある。
- 「ウ　アカウンタビリティ関係」について、AI ガバナンスを含む内部統制システムの適切な運用・維持は重要だが、既存の承認プロセスを超えた新たな AI 専用の文書化は、経営資源を圧迫し、開発スピードを著しく阻害するおそれがある。上場企業においては、事業報告や内部統制報告書等を通じて、権利者・ユーザー・投資家といった各ステークホルダーに対し、既に透明性のある適切なガバナンス情報の開示を行っている。こうした既存の開示の枠組みによってステークホルダーへの説明責任は十分に果たし得るため、新たな文書化を課さずとも、これらの手段による代替可能性を認めていただくことで実務上も特段の問題は生じないと考えられる。したがって、ISMS や上場企業としての既存の内部統制プロセス等との整合性を図り、追加的な実務負担を最小限に抑えるべき。既存の法令上の要請に従った範囲に留めるような制度設計を考えるべき。
- 「ア　使用モデル」について、SaaS 事業の現場においては、顧客への価値提供を最適化するため、一つのサービス内で複数の生成 AI モデルを組み合わせたり（マルチモデル）、機能改善のために短期間でモデルを入れ替えたりすることが一般的である。本プリンシプル・コード案において示された「すべてのモデル」の概要開示を一律に求めることは、以下の観点から実務上の合理的範囲を超え、事業活動に支障をきたす懸念があることから、使用モデルの内容や数

などを限定するなど、開示内容を限定すべき。また、現時点で想定している、使用モデルに関する開示内容の粒度、範囲又は内容（例：使用しているモデルのすべてか／サービスごとか／利用数の上位のみか等）を明らかにすべき。

1．競争優位性（営業秘密）の保護：

どの機能をどのモデルのどのバージョンで実装し、どう組み合わせているかという「構成（アンサンブル）」自体が、事業者の重要な差別化要因となる。たとえ概要であっても、全モデルの開示を求めることは、競争上の機微な情報の流出を招き、公正な競争環境を阻害するおそれがある。

2．実務負担の増大と情報の形骸化：

開発初期の試行的なモデルや、補助的な一部機能にのみ利用される特定モデルまで網羅的に確認・公表・更新し続けることは、多大な事務的コストを伴う。これはスピードが求められる AI 開発サイクルを停滞させ、結果として「開示のための開示」という形骸化を招くリスクがある。

3．利用者視点での最適化：

利用者にとって実益があるのは、サービス全体のガバナンス体制や、主要な機能がどのように管理されているかという情報。したがって、開示対象については「利用数や事業への寄与度が一定以上の主要モデル」に限定する等の、リスクベース・アプローチに基づく具体的なガイドラインを示すべき。

以上より、使用モデルの内容や数などを限定することを求めるとともに、個別のマイナーモデル詳細を逐一開示するのではなく、例えば、主要モデルに絞った適切な開示と、サービス全体の「モニタリング体制や AI 倫理への対応状況」といったガバナンス体制の開示をもって、透明性を確保する手法を認めるべきと考えており、このような制度設計を追求すべき。

（2）知的財産権保護のための措置

- 実務及び海外での先行事例の観点から、以下の 2 点を要望する。

1．技術的な対応状況の公表範囲の適正化：EU AI Act 等の海外の事例においても、著作権保護に関するポリシー策定や学習データの要約公開は求められているものの、個別の技術的な措置に関する詳細な「対応状況」の一般公表までは義務付けられていない（これらは主に規制当局向けの技術文書等の枠組みで扱われるか、事業者の自律的な運用に委ねられている）。

これに対し、本コード案が、事業者が提供する全てのサービスについて、個別に詳細な著作権保護に関する対応状況を確認し、広く一般に公表することを求めることは、過大な事務負担を招き、事業成長を阻害する懸念がある。ひいては、わが国の AI 産業の発展を阻害する可能性もあるものと考える。

したがって、公表範囲については、先行する海外の事例と同様に「著作権保護に関する基本ポリシー」及び「ポリシーの定期的な見直し状況」や「窓口の設置」等の基本事項に留め、技術的な詳細の公表については慎重であるべきではないか。なお、EU AI Act 第 53 条に基づく「Code of Practice」においても、著作権法遵守の体制構築（Measure 1.1 等）

は求められているが、その技術的な詳細仕様についてまでの対外的な公表は必須とされていない。わが国の制度設計においても、こうした海外の動きと足並みをそろえ、実務上の配慮をすべきである。

２．ガバナンス体制に基づく自律的な運用の尊重：

ポリシーの遵守状況の確認手法やモニタリングの結果は、各事業者の内部管理手法そのものであり、競争上の機微な情報に該当する。これらを詳細に外部公表することは、かえって事業者の管理体制の脆弱性を露呈させる等のセキュリティリスクに繋がる懸念がある。本プリンシパルコードにおいて、透明性の確保は「管理体制の有無」や「基本方針」の公表をもって足るとし、具体的な運用の詳細は各事業者の自律的なガバナンスに委ねるという理解で相違ないか。実効性のあるガバナンスを維持するためにも、事業者の自律性を尊重する運用の徹底を要望する。

- そもそも robots.txt は、サーバー負荷の分散等を目的とした技術的なプロトコル（通信上の作法）であり、著作権保護を目的としたものではない。これを著作権保護の主要手段として絶対視することは、技術の本来の用途を超えた制約に繋がる懸念がある。機械可読な指示を一律の制限とせず、その設定目的（負荷分散等）に応じた柔軟な取り扱いを認めるべき。
- ユーザーが自らの意思で同意し、利便性向上のために望むデータ連携（家計簿サービス等）までもが、画一的なクローラ規制によって阻害されることは避けるべき。機械可読な指示の遵守と、ユーザーの明示的な意向に基づく適正なデータ活用を、どのように両立・調和させていくべきと議論されているのか。また、ログの記録・保存についても、事業者に過度な負担とならぬよう、経済的に合理的な範囲に限定されることを要望する。

（細則）

- 2 点目に「概要開示対象事項の具体例を参照されたい」との記載があるが、実務上の観点からみると、情報の粒度が細かくなるほど、毎年の更新作業における社内確認コストや実務負担が大幅に増大するため、変化の激しい AI 分野において、過度な開示・更新を課すことは、かえって情報の形式化や開発サイクルの停滞を招くおそれがある。また、政府当局が参考様式やひな型を提示する場合、それが事実上の「最低基準」として機能し、本来「概要」で足りるはずの項目についてまで詳細な開示を事実上強制するリスク（レピュテーションリスクを含む。）がある。あくまで「コンプライ・オア・エクスプレイン」の趣旨に則り、各事業者が自社のリスクや機密保持の必要性に応じて、開示の粒度を合理的に判断できる柔軟な運用を担保すべき。具体的には、一律に詳細な開示を求めるような「ひな形」の提示ではなく、秘匿すべき情報（営業秘密等）に配慮した上での「好事例」を例示するなど、事業者が納得感を持って開示内容を選択できるような指針の策定を要望する。

【原則２】

- 原則２や３に基づく個別の開示請求への対応は、対応体制の構築を含め、事業者に膨大な工数を強いることとなるが、特にリソースが限られたスタートアップにとって、スピード感を持った開発は生命線である。開示対応に伴う負担増は、本来集中すべき技術革新を阻害し、競争力

を削ぐ大きなリスクとなることから、事業規模やリソースを考慮し、スタートアップに対しては、開示義務の段階的な適用や、簡便な対応プロセスの策定など、開発スピードを損なわない具体的な配慮を強く求める。

- 「開示要求者」に関する新たな情報提供スキームを新設するのではなく、権利者救済や証拠収集に関しては、原則として既存の法的手続（裁判所の関与の下での手続等）に委ねる方向で整理すべきと考える。少なくとも、回答を要請し得る場面に関しては法令に基づく正式な手続きがある場合等に限定するなど、濫用抑止と事業者負担の適正化を明確にすべき。具体的には、開示請求への回答義務（または努力義務）の例外として、「法令上の守秘義務（弁護士法、公認会計士法等）を負う専門職が利用・提供する場合」や「契約上の秘密保持義務に抵触する場合」を明記し、既存の保護法益を侵害しないこと等を担保すべき。特にリーガルテック分野は、利用者が紛争当事者や代理人である場合も多く、開示請求対応が常態化した場合の運用コストが極めて大きい。また、照会に用いられる生成物・プロンプト等には、当事者の機微情報や法的戦略が含まれることがあり、照会対応そのものが新たな漏えい・紛争リスクになり得る。法務領域においても、弁護士法第 23 条等に基づく高度な守秘義務が課された情報も含まれる可能性があり、本コードに基づく任意の開示請求に応じることが、これら法令上の義務と衝突し、弁護士等の利用者がコンプライアンスジレンマに陥る懸念がある。さらに、本案が想定する情報提供が、訴訟準備段階での情報収集として機能すると、既存の裁判手続上の情報収集制度との二重化・迂回を招き、当事者間の衡平や濫用抑止の観点でも問題が生じ得る。結果として、国内での提供回避や新規参入の抑制につながり、利活用促進という政策目的に反するおそれがある。
- 「開示要求可能事項」について、民事訴訟法には、当事者照会（163 条）や文書提出命令（221 条等）といった、裁判所の関与と厳格な規律の下での証拠収集手続が確立されている。ソフトローである本プリンシプル・コードにおいて、紛争当事者の一方が相手方に不利益な資料又は情報（「【開示要求可能事項】」における「自らが照会を行うＵＲＬ等の情報」）を直接提出させる仕組みを設けることは、これら司法上の適正手続を実質的に回避・代替させることになりかねない。したがって、原則２に基づく開示範囲は、「原則２開示要求者」が司法手続において対象文書を特定するために必要最小限の情報に留め、資料又は情報そのものの開示は裁判所が判断する司法手続に委ねるべき。また、本件について、原則２の趣旨を明らかにし、開示対象に資料や文書そのものの開示は含まれない旨を明確化すべき。
- 「開示の求めが満たすべき事項」に関し、クローリング対象の URL やデータセットの詳細は、どのウェブサイトからどのようなデータを収集・加工したかという、事業者の重要なコア技術やノウハウそのものであり、事業者の正当な利益として保護されるべきもの。これらが明らかになることは、事業者の技術的優位性を根底から損ない、ひいては、事業者間の健全な競争が働かなくなるおそれがある。
- 「開示の求めに係る回答の利用目的が明示されており、かつ、原則２開示要求者が当該目的以外の目的で利用しない旨を誓約していること」として、目的外での利用について誓約していることが条件となっているが、司法上の要請であれば一定の権利や利益を保護する手続・罰則などもあるところ、ソフトローに従って誓約書を回収したのみでは、目的外利用がなされた場合

に損害の補填を行うことができない可能性がある。また、提出された文書に「営業秘密」が含まれる場合は、裁判所への申立てにより「秘密保持命令（民事訴訟法 133 条)」を求めることができる司法手続と比較し、秘密を保持する実効性にも欠けるものと考える。したがって、一度の流出が不可逆的な損害に繋がりかねない技術的ノウハウ等については、事業者の正当な利益を保護する観点から、回答拒否が認められることを明文化すべき。

- 「【開示要求可能事項】」及び「(細則)」の 6 点目において体制整備への言及があるが、生成 AI 提供者において、既存の生成 AI 開発者が開発している生成 AI モデルを提供している場合については、生成 AI 開発者が開示しているような事項を生成 AI 提供者が開示することは、重複した開示になると考える。また、生成 AI 開発者が開示していない事項を生成 AI 提供者が開示することについても矛盾があると考えられる。生成 AI 提供者と生成 AI 開発者では、開示すべき項目の範囲や体制整備に求められるレベルを明確に分けるべき。

（細則）

- １点目について、生成 AI 事業者が原則 2 開示要求者を「該当する者であることを示す理由」の提示を求める旨が記載されているが、この判断基準が曖昧な場合、十分な法的根拠を欠いた「情報収集目的」の探索的な請求（フィッシング・エクスペディション）を許容するリスクがある。
- 企業の知的財産やノウハウを不当な流出から守る観点から、「該当する者であることを示す理由」の正当性は生成 AI 事業者の裁量によって判断できるものであり、客観的な疎明（弁護士による受任通知や具体的準備状況を示す書面等）がない場合には当該事業者の判断で回答を拒否できるという理解である。この理解に齟齬があるようであれば理由を提示して頂きたい。

【原則３】

- 原則２や３に基づく個別の開示請求への対応は、対応体制の構築を含め、事業者に膨大な工数を強いることになるが、特にリソースが限られたスタートアップにとって、スピード感を持った開発は生命線である。開示対応に伴う負担増は、本来集中すべき技術革新を阻害し、競争力を削ぐ大きなリスクとなることから、事業規模やリソースを考慮し、スタートアップに対しては開示義務の段階的な適用や、簡便な対応プロセスの策定など、開発スピードを損なわない具体的な配慮を強く求める。(再掲)
- 「開示要求可能事項」について、民事訴訟法では、当事者照会（163 条）や文書提出命令（221 条等）といった裁判所の関与と厳格な規律の下での証拠収集手続が確立されている。ソフトローである本プリンシプル・コードにおいて、紛争当事者の一方が相手方に不利益な資料又は情報（「コンテンツ（中略）が掲載されたＵＲＬ等の情報」）を直接提出させる仕組みを設けることは、これら司法上の適正手続を実質的に回避・代替させることになりかねない。したがって、原則３に基づく開示範囲は「原則３開示要求者」が司法手続において対象文書を特定するために必要最小限の情報に留め、資料や文書そのものの開示は裁判所が判断する司法手続に委ねるべき。また、本件について、原則３の趣旨を明らかにし、開示対象に資料や文書そのものの開示は含まれない旨を明確化すべき。

- 「開示の求めが満たすべき事項」について、クローリング対象の URL やデータセットの詳細は、どのウェブサイトからどのようなデータを収集・加工したかという、事業者の重要なコア技術やノウハウそのものであり、これらが明らかになることは、事業者の技術的優位性を根底から損ない、ひいては、事業者間の健全な競争が働かなくなるおそれがある。
- 「開示の求めに係る回答の利用目的が明示されており、かつ、原則 3 開示要求者が当該目的以外の目的で利用しない旨を誓約していること」として、目的外での利用について誓約していることが条件となっているが、司法上の要請であれば、一定権利利益を保護する手続・罰則などもあるところ、ソフトローに従って、誓約書を回収したのみでは、目的外利用をされた場合には損害の補填を行うことができない可能性がある。また、提出された文書に「営業秘密」が含まれる場合は、裁判所への申立てにより、「秘密保持命令（民事訴訟法 133 条）」を求めることができる司法手続と比較し、秘密を保持する実効性にも欠けるものと考える。したがって、一度の流出が不可逆的な損害に繋がりかねない技術的ノウハウ等については、事業者の正当な利益を保護する観点から、回答拒否が認められることを明文化すべき。
- 「【開示要求可能事項】」及び「（細則）」の 6 点目において体制整備への言及があるが、生成 AI 提供者において、既存の生成 AI 開発者が開発している生成 AI モデルを提供している場合について、生成 AI 開発者が開示しているような事項を生成 AI 提供者が開示することは、重複した開示になると考える。また、生成 AI 開発者が開示していない事項を生成 AI 提供者が開示することについても矛盾があると考えられる。生成 AI 提供者と生成 AI 開発者では、開示すべき項目の範囲や体制整備に求められるレベルを明確に分けるべき。

（細則）

- 2 点目で「生成 AI 事業者において可能な限り詳細かつ分かりやすい開示を行う」ことが求められているところ、原則 2 とは異なり、「開示要求者に該当する者であることを示す理由」として「生成物及び当該生成物を生成する際に用いたプロンプト」の提示を求める旨が記載されているが、実際に生成 AI に関するコンテンツ利用者か否か（第三者の権利侵害の可能性がある者か否か）を判断するには不十分な例示であると考える。このように、判断基準が曖昧な場合、十分な法的根拠を欠いた「情報収集目的」の探索的な請求（フィッシング・エクスペディション）を許容するリスクがあるのではないか。また、URL 等の詳細は重要な技術的ノウハウであると同時に、開示によってセキュリティ上の脆弱性を露呈させる懸念もある。企業の知的財産やシステムの安全性を守るためには、開示の是非について生成 AI 事業者自身が適切な裁量をもって判断できること、及び、第三者の権利侵害を起こしてしまう蓋然性を示す客観的な疎明がない場合には回答の拒否を行えること等を明確化すべき。
- 特定の URL が学習データに含まれるか否かの照会回答については、原則 2 に関する要望と同様に、事業者の知的財産権や営業秘密・ノウハウの保護及びセキュリティ確保の観点から、生成 AI 事業者の裁量により回答拒否を認める旨を明記することを強く要望する。
- 細則に示された特定の URL が学習データのクロール対象か否かという情報は、生成 AI 事業者にとって「どのようなソースから、どのような優先順位でデータを収集・精査しているか」という技術的優位性の根幹（ノウハウ）を特定させる行為に他ならない。不特定多数になり得る

利用者からの URL 照会に対し、一律に回答を求める運用は、リバースエンジニアリングによる営業秘密の流出や、攻撃のヒントを与えることによるセキュリティ上の脆弱性の露呈を招くおそれがある。また、目的外利用の「誓約」のみでは情報流出時の不可逆的な損害を補填・回復する実効性に欠けると考えられる。このような重大な実務上のリスクに鑑みれば、開示によって事業者の正当な利益やシステムの安全性が害されるおそれがある場合には、事業者の裁量によって回答拒否が認められるべきと考える。この理解に齟齬があるようであれば理由を提示頂きたい。

（2）この文書が示す原則に対する例外、について

- 「【原則 1 から原則 3 までに対する例外】」が記載されているが、自社開発ではないオープンソースソフトウェア（OSS）モデルや公開リポジトリを利用する場合、開発過程の詳細を遡及して把握・精査することは技術的に困難であることから、OSS ライセンスの提示をもって内容の開示に代えることができるとする例外規定について、実務の実態に即した柔軟な運用を要望する。
- 生成 AI の開発・提供において、OSS の活用はイノベーションを加速させる不可欠な要素である。しかし、OSS は不特定多数のコントリビューターによって構築されており、利用側である事業者がそのトレーニングプロセスの詳細や学習データの全容を遡及的に完全把握し、保証することは物理的に不可能。開発主体が異なる OSS について過度な情報開示や遡及的な説明責任を課すことは、実質的に OSS の利用を制限することに繋がり、わが国の AI 産業の発展を阻害するおそれがある。OSS 利用の事実とライセンス情報の提示をもって原則への対応とみなす本例外規定は、実務上の実現可能性を担保する上で極めて重要であり、一律の基準ではなく、個別の技術的背景を考慮した柔軟な運用を求める。

（4）その他の事項

- 本プリンシプル・コードへの対応は、事業者にとっては人的・技術的・経済的に多大なコスト（コンプライアンス・コスト）を伴うものだが、これを単なる「一方的な負担」に留めず、前向きな投資へと変えるための具体的な枠組みが必要であると考える。
- 「期待される」との表現に留めることは、実効性確保に関する政府の責任の明確化という観点から不十分ではないか。中小規模の事業者も対応負担を上回るメリットを享受できる仕組みとすることで、日本全体の AI ガバナンスの底上げを図るべき。この点について、例えば、準拠事業者に対する政府調達における優先的な評価や、認定マークの付与、あるいは ESG 評価との連携に加え、本案への準拠及び届出を行った事業者を「好事例集」として政府が対外的に公表・周知するなど、実質的なインセンティブを設計・提示される予定は今後あり得るのか。このような実効的なメリットを明示することは、リソースの限られた中小規模の事業者の自発的な体制整備を後押しし、わが国の AI 利活用における安全・安心の底上げに寄与すると考える。

（その他、全般に関する意見）

- 今後、インターネット上に重要なデータは存在しなくなる可能性もあり得る。また、生成 AI が進化すると目的特化型の AI の世界が来るものと考えられる。日本が狙うべきはヘルスケア領域だが、AI のベースとなるデータは個人のデータとなるため、個人のデータをルールなく活用していく AI が乱立すると、データの真正性や秘匿性が保たれなくなる可能性が高い。まずは、ヘルスデータは個人のアセットであり、どこに利用を許可したかどうかをブロックチェーンで追える（トレースできる）基盤が必要不可欠であり、それがないと真正性の保たれない情報が流通し、AI が本来の力を発揮できなくなる可能性があり得る。加えて、現在流通している匿名加工されたヘルスデータも、本当に真正性を保てているのかが不透明。個人のアセットを個人が管理し、いつでもトレースできる情報保護基盤がないままでは、目的特化型の AI をヘルスケア領域で深化させることはできないばかりか、正確ではない AI が出来てしまう可能性が非常に高いことを危惧する。
- 概要開示対象事項 具体例の 3 ページに関して、オリジナルの権利者に配慮した「合成データの活用」や「クリーンなデータセットによる学習」を採用している事業者については、その取組を公的に高く評価すべき。また、知的財産権の保護に積極的に寄与する学習手法をとっていると認定された事業者に対しては、インセンティブとして原則 1 から 3 までに示された公開レベルを軽減する（簡易的な開示や説明で充足とする等）といった処置を検討すべき。このような軽減措置があれば、事業者は積極的に権利配慮型の手法を選択するようになり、本コードの目的である「知財保護と技術進歩の両立」がより円滑に達成されると考えられる。
- 本プリンシプル・コード案は、知的財産等の権利者保護という便益に対し、AI 開発・提供事業者に課されるコスト（過大な事務負担や AI 活用の萎縮効果）が著しく不均衡であり、『世界で最も AI を開発・活用しやすい国を目指す』という政府の国家戦略との整合性に重大な疑義がある。 AI 活用は日本産業の国際競争力において不可欠な要素である。日本国内でサービスを展開する企業にのみ独自の制約を課すことは、国際競争における致命的なハンディキャップとなり、国家戦略上の合理性を欠いている。具体的には、「推論過程や判断根拠」を含む「モデルのトレーニングプロセスの内容」や「第三者と契約するライセンスの状況」を公表することは AI 事業者にとっての「手の内（知財そのもの）」を無償で公衆に晒すことに等しく、国際的な開発競争において致命的な不利益を招く。これは、本来守られるべき「AI 開発・提供者側の知的財産」を軽視したバランスを欠く要求である。
- 各国で規制が断片化することは、グローバル企業にとって多大なコンプライアンス・コストを発生させる。日本独自の基準を設けるのではなく、広島 AI プロセス等の国際枠組みへの準拠に集約すべきである。国際的な整合性を欠いた規制は、日本市場の孤立を招き、国内企業の競争力を削ぐ要因となりえる。
- AI 推進法の付帯決議においても、「過度に重い負担や情報開示を求めないように留意すること」、「広島ＡＩプロセス国際行動規範の『報告枠組み』に基づき報告書を提出する活用事業者等に対しては、既存の国内法制度に基づく報告義務に最大限活用することで、報告の重複を軽減する仕組みを導入することなどにより、国際的な整合性や効率性を確保すること。」とされており、本コードにおけるフレームワークを新たに導入することはこの付帯決議の内容に反す

る制度設計である。

- 生成 AI の開発・提供において、透明性の確保は重要な要素であることは認識しているが、本プリンシプル・コードの策定にあたり、マルチステークホルダープロセスを重視し、知的財産の権利者等だけでなく AI 開発・利用企業とも実行可能な記載等について事前に対話を行っていれば、企業側もより柔軟に対応ができた可能性がある。今後は業界団体等を通じて事前の意見交換等を実施する等、制度設計プロセスの改善をいただきたい。
- 本プリンシプル・コード案は「知的財産の保護」を掲げているが、示されている具体的措置の多くは権利者の救済にとって手段と目的が乖離しており、実効性に欠けていると考える。
  原則 1 で求められている「アーキテクチャ・設計仕様」や「パラメータの設定（判断根拠）」等の開示は極めて内部的な技術情報である。これらの情報が公表されたとしても、個別のクリエイターが自らの著作権侵害を特定したり、法的立証を行ったりすることには直接寄与しない 。IP ホルダーが求めているのは、自身の作品が「学習に使われたか」という事実の確認や「侵害物の生成防止」であり、システムの内部構造の透明性ではないものと思料する。この点において、本プリンシプル・コード案は、権利者への実効的な救済手段を提供するのではなく、事業者側に「説明のための説明」という形式的な事務負担を強いるものとなっている。
  （「情報の開示」と「権利行使」の論理的断絶）
  原則 2 及び 3 は、権利者が自ら類似性を発見し、訴訟準備等の高いハードルを越えた場合にのみ開示を求める仕組みとなっている。これは権利者にとって依然として負担が重く利用されるケースが少ないことが予想される一方、AI 事業者側にのみ膨大な窓口対応コストを強いる、非効率な対症療法に留まっている。（事後的な照会プロセスの限界）

以　上