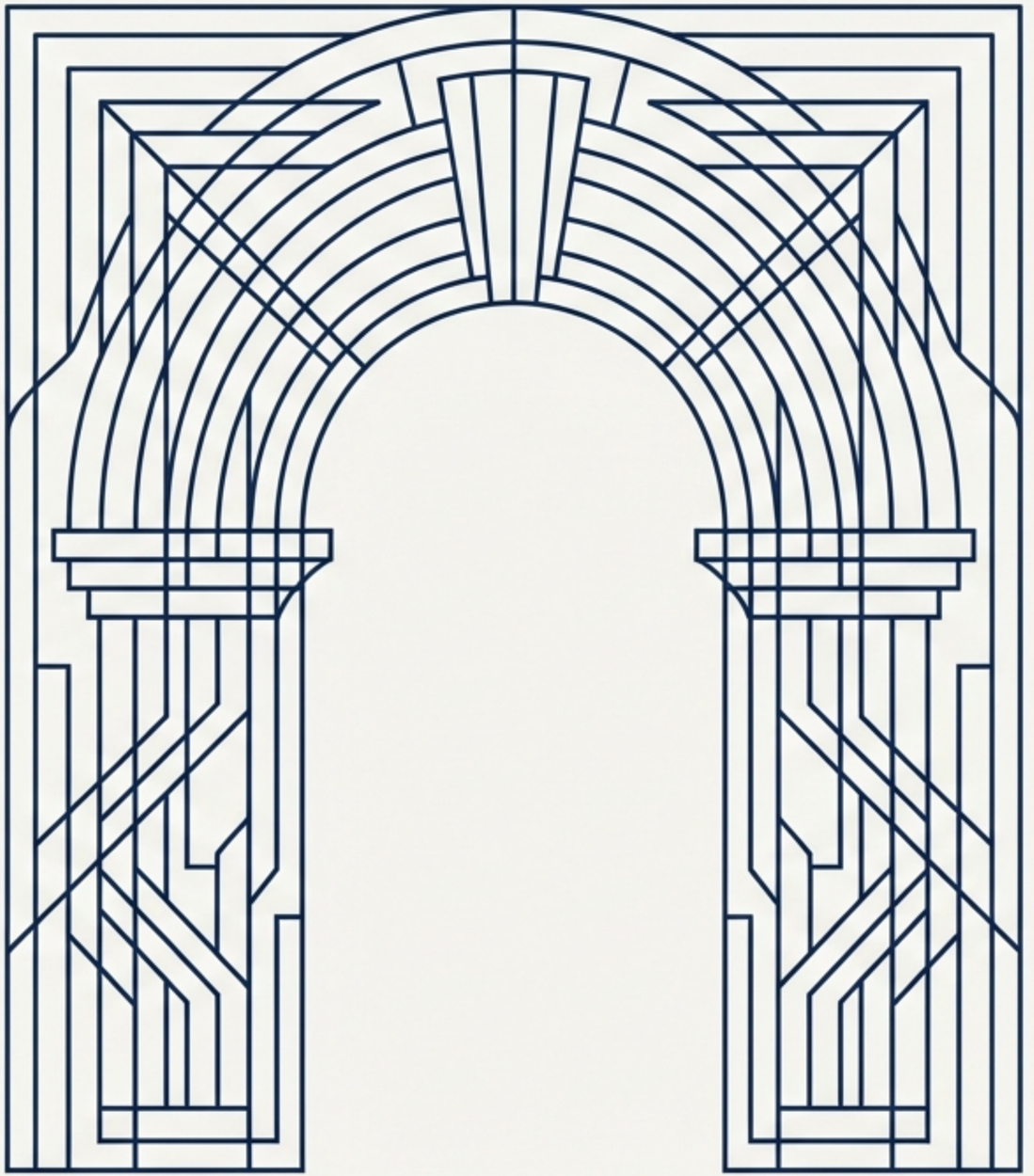
シラバス2026年試験対応

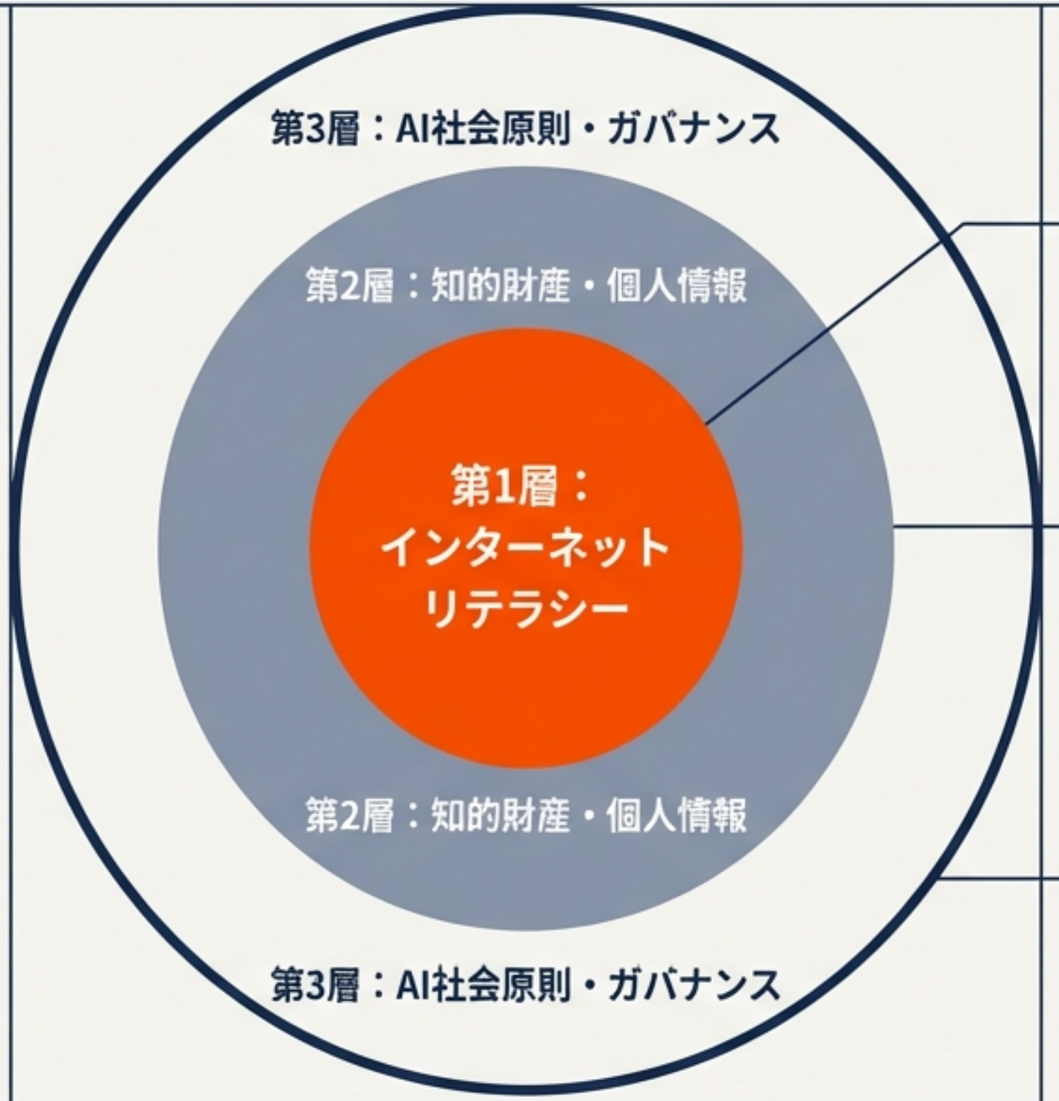
生成AIパスポート試験 第4章 要点まとめ

情報リテラシー・法的枠組み・AI社会原則

Chapter 4: Comprehensive Summary



AI時代を生き抜くための3つの知識層



Act I (Center):
技術や脅威を理解し、自身を守る

Act II (Middle):
著作権やプライバシーなど、他者の権利を侵害しないための法知識

Act III (Outer):
人間中心の社会を維持するための倫理とガイドライン

インターネットリテラシーの4要素

定義：インターネットに関わる技術、ルール、脅威を理解し、適切に使用できる知識や能力

1. テクノロジーの理解

時代の流れに合わせてテクノロジーを把握する能力

2. 情報リテラシー

特定の情報を見つけ、判断し、活用する能力

3. セキュリティとプライバシー

データやプライバシーを外部から守る手段を知り、実践する能力

4. デジタル市民権

情報を効果的に見つけ、創造し、倫理的で責任ある行動をとる能力

デジタル空間の脅威：技術的攻撃と心理的攻撃

技術的脅威（Technical Threats）

- **フィッシング詐欺:** メールやWebを通じた情報の不正収集
- **スミッシング:** SMSを使ったフィッシング
- **QRコード詐欺 (Quishing):** 悪意あるQRで不正サイトへ誘導
- **マルウェア:** 偽Wi-Fi接続や不適切なDLによる感染
- **ランサムウェア:** データを暗号化し「人質」にして身代金を要求

ソーシャルエンジニアリング（Human Hacking）

人間の心理的・感情的な隙をついて情報を盗む手法

- **スピアフィッシング:** 特定の個人・組織を標的化
- **ベート攻撃（Baiting):** 魅力的なコンテンツを「餌」にする
- **プレテキスト:** 虚偽のシナリオ（身分詐称など）で騙す
- **ブラックメール:** 秘密の暴露を脅迫材料にする

防御メカニズム：セキュリティ対策の基本

ソフトウェア対策
アンチウイルスソフトを最新状態に保つ。定期的なシステムスキャン。

通信の保護
偽Wi-Fiを避け、信頼できるネットワークのみ接続。

データ管理
アップロード時の情報漏洩（個人情報・機密情報）とダウンロード時の感染リスクを理解する。

プライバシー設定
SNS等で自分の情報へのアクセス範囲を制限（意図しない収集を防ぐ）。

パスワード管理
推測されにくいパスワードの使用と多要素認証。

個人情報保護法と取扱事業者の責務

個人情報（Personal Info）
特定の個人を識別できるもの（氏名、生年月日、個人識別符号など）。

要配慮個人情報（Sensitive Personal Info）
人種、信条、病歴、犯罪歴など。
⚠ 原則、事前の本人同意が必要。

匿名加工情報
特定個人を識別できず、復元できないように加工した情報。

重要定義：個人情報取扱事業者

個人情報データベース等を事業（営利・非営利問わず）の用に供している者。

※改正により、取り扱う情報の数に関わらず対象となる（「5000人分以下なら対象外」は撤廃済み）。

生成AIにおける個人情報の取り扱いルール

INPUT（入力）

- 目的達成に必要な範囲にとどめる（最小化）
- 利用目的を超えて利用する場合は、事前に本人の同意を得る
- 機微（センシティブ）情報は機微（センシティブ）情報は原則入力しない ⚠

GENERATIVE AI（生成AI）

OUTPUT（出力）

- 不正な第三者提供にならないよう管理する
- 不正な第三者提供にならないよう管理する
- 生成物に他人の個人情報が含まれていないか確認する

MANAGEMENT（管理）

保管・廃棄時には適切なセキュリティ対策（削除・溶解等）を講じる。

知的財産権の全体像

著作権 (Copyright)	特許権 (Patent)	意匠権 (Design)	商標権 (Trademark)
			
著作物（思想・感情の創作的表現）	発明（高度な技術的アイデア）	物品・画像のデザイン（形状・模様・色彩）	事業者の識別マーク（ロゴ、ブランド名）
登録不要で発生（無方式主義）	産業の保護と利用	美観を起こさせるもの	創作ではなく「使用」による信用を保護 AI生成商標も保護対象

生成AIと著作権：「創作的寄与」の壁

Q: 人の「創作的意図」と「創作的寄与」があるか？

YES

著作物として認められる

AIを利用者が道具として使用。
→ 利用者が著作者。

NO

著作権は発生しない

AIが自律的に生成 / 人は指示のみ。
→ 日本の現行法の解釈。

⚠ 侵害リスク（Infringement）

既存の著作物に「依拠」し、「類似」している生成物を利用すると、著作権侵害になる可能性がある。

※特許・意匠も同様に、人の関与がなければ権利は認められない。

肖像権・パブリシティ権・不正競争防止法

肖像権 (Portrait Rights)

実在する人物の顔・姿（生成画像を含む）を無断で使用・公表されない権利。
プライバシー保護（幸福追求権）。

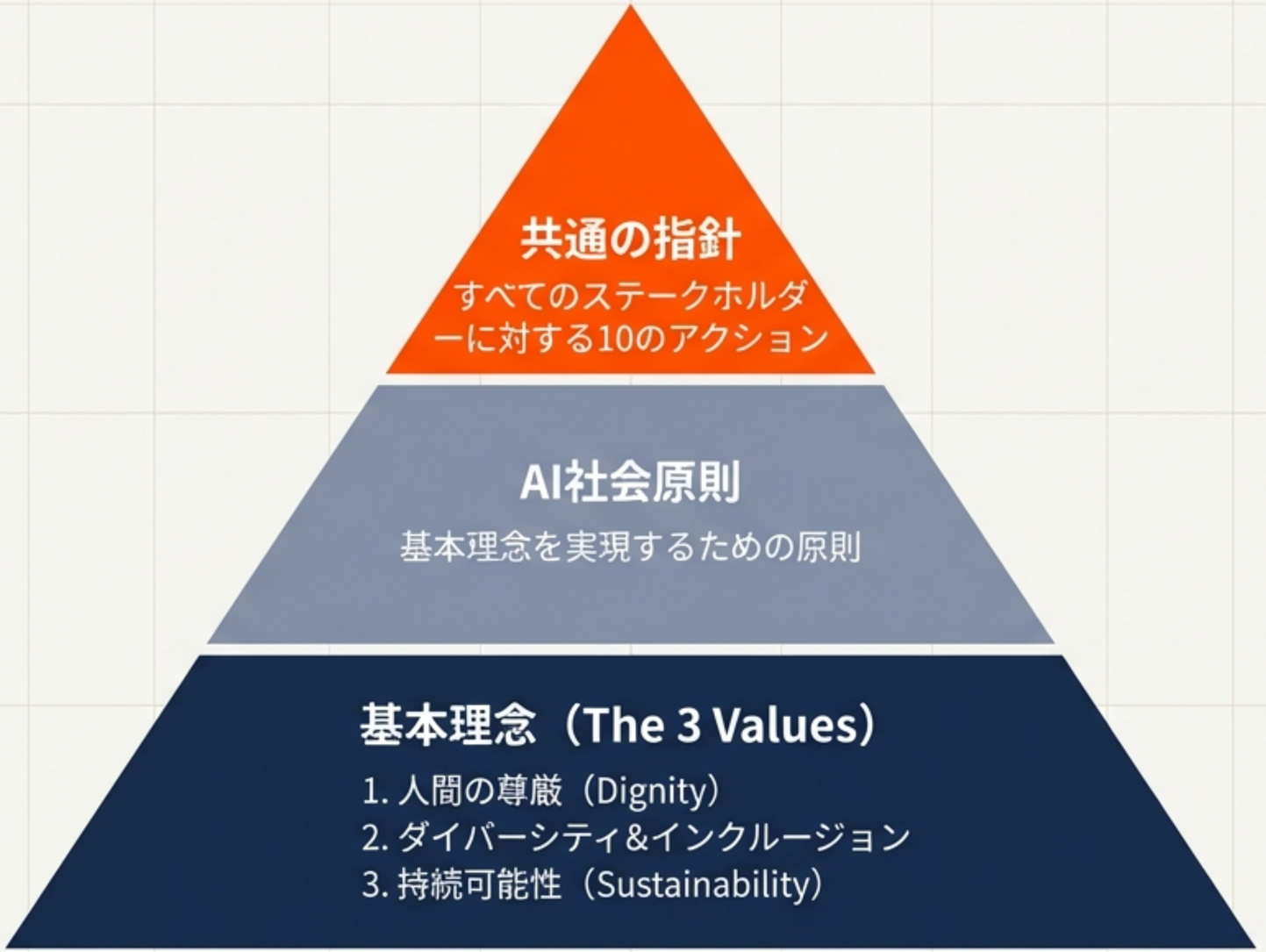
パブリシティ権 (Publicity Rights)

著名人の氏名・肖像が持つ「顧客吸引力（経済的価値）」を排他的に利用する権利。
無断で広告利用することはNG。

不正競争防止法 (Unfair Competition)

- 混同惹起: 他社のブランドと誤認させる
- 営業秘密侵害: 秘密をAIに入力・利用
- 限定提供データ: データの不正利用

AI社会原則のピラミッド構造



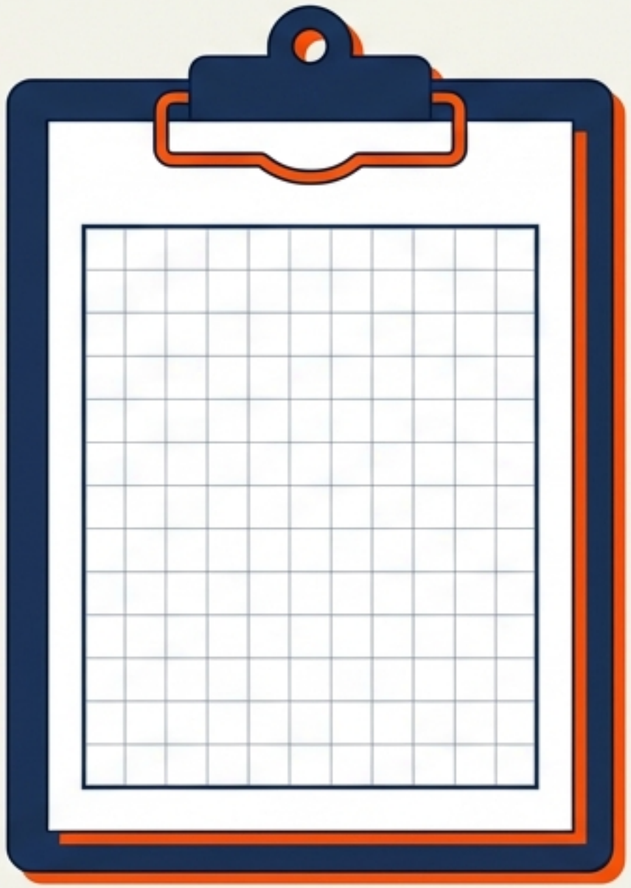
AI事業者ガイドライン：共通の指針

1. 人間中心	2. 安全性	3. 公平性	4. プライバシー保護	5. セキュリティ確保
6. 透明性	7. アカウンタビリティ	8. 教育・リテラシー	9. 公正競争確保	10. イノベーション

AIシステム・サービスを開発・提供・利用する全ての主体が留意すべき事項。

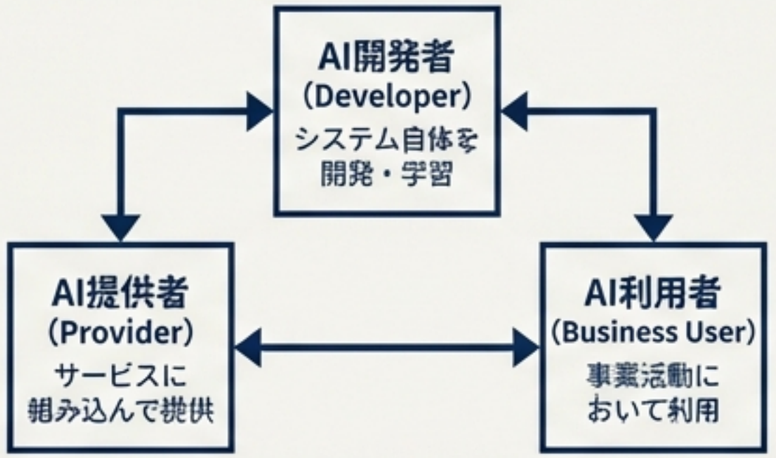
高度なAIシステムに関係する事業者の追加義務

共通の指針に加え、以下の高度な対策が求められる

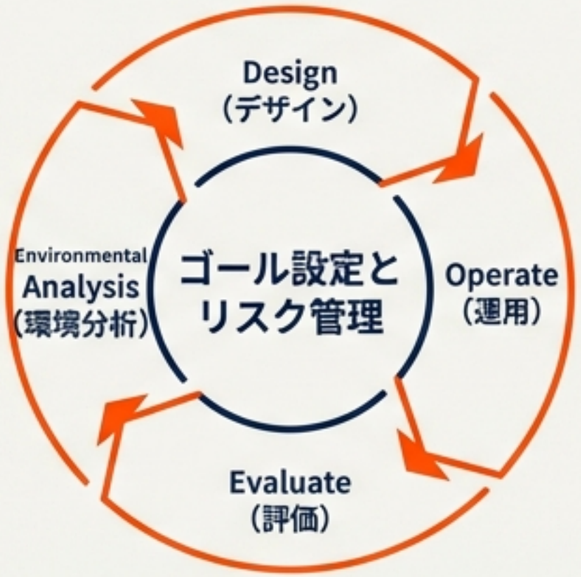


- ☐ リスク管理: ライフサイクル全体のリスク評価（レッドチーミング等）
- ☐ 脆弱性対策: 市場投入後のインシデント特定・緩和
- ☐ 透明性: 能力・限界の公表
- ☐ 電子透かし: AI生成コンテンツ識別技術（Origin/Provenance）の導入
- ☐ 情報共有: 産業界・政府・学界でのインシデント報告
- ☐ 優先的投資: 社会的安全、気候危機などの課題に対する開発

AIビジネスの3つの主体とガバナンス



ガバナンス・サイクル（Governance Cycle）



AI新法（2025年）：イノベーションと規制のバランス

2025 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

基本理念

- イノベーションの促進 + リスク対応
- ソフトロー基点（自主性と協力義務）
- 内閣に「AI戦略本部」を設置

事業者の義務

- 基本理念に沿った活用の「努力義務」
- 高リスクAIには、より強い義務が課される可能性

Takeaway:
法的拘束力のないガイドラインから、法的根拠のある「協力義務」への移行。