ISACA.AAIA.v2026-11-09.q201

試験コード：	AAIA
試験名称：	ISACA Advanced in AI Audit
認証ベンダー：	ISACA
無料問題の数：	201
バージョン：	v2026-11-09
ページの閲覧量：	106
問題集の閲覧量：	2032

https://www.jpnshiken.com/shiken/ISACA.AAIA.v2026-11-09.q201.html

質問: **1**
IS監査担当者が、生成型AIが同じデータセットから異なる投資推奨を返す可能性があることを認識しておくべき主な理由は、次のうちどれですか？
A. リスクプロファイルの定量化には限界が生じる可能性があります。
B. ニューラルノードへのアクセスは、プロセスが実行されるたびに変化します。
C. 計算論理は確率に基づいています。
D. サーバーは定期的に再構成されます。
正解: **(**正解を表示します**)**
生成型AIシステム、特にトランスフォーマーモデルに基づくシステムは、確率的計算を用いて出力を生成します。そのため、同じ入力データが与えられた場合でも、サンプリング戦略（例えば、温度、トップkサンプリング）によって異なる出力が生成されることがあります。
「生成型AIは確率的に動作するため、確率的サンプリング手法に基づいて、実行ごとに出力が変化する可能性があります。この変動性は想定内のことであり、金融などのリスクに敏感な環境では考慮に入れなければなりません。」

質問: **2**
ある小売企業は、顧客の購買傾向に基づいて在庫を予測するためにAIモデルを使用し、四半期ごとにモデルを更新しています。このモデルは最近、人気の高いショッピングシーズン中の需要の急増を認識できませんでした。この状況は、次のうちどの問題を最もよく示していますか？
A. データセットの多様性が限られているため、モデルトレーニングに影響が出ている
B. データドリフトがシステム予測に与える影響
C. 訓練データセットが小さいため、過学習の問題が発生する。
D. 予測精度に影響を与えるデータの外れ値チェックの欠如
正解: **(**正解を表示します**)**
データドリフトとは、入力データの統計的特性が時間とともに変化し、AIモデルの精度に影響を与える現象です。今回のケースでは、モデルが最近の需要動向に適応できなかったため、学習に使用したデータが現在の状況を反映していないことを示しています。

データドリフトは、現実世界の入力データが訓練データのパターンから逸脱すると、AIシステムの性能低下につながります。特に小売業のような動的な環境では、データドリフトの監視が不可欠です。」

質問: **3**
ある組織が、顧客アカウントから収集した情報を使用してAIチャットボットをトレーニングしています。この方法に伴う最大のリスクは次のうちどれですか？
A. 透明性
B. 個人情報の開示
C. AIバイアス
D. AIモデルの幻覚
正解: **(**正解を表示します**)**

質問: **4**
AIシステムのコンプライアンスを監査するための最適なアプローチは次のうちどれですか？
適用されるプライバシー規制における「説明を受ける権利」とは？
A. 組織が個人に重大な影響を与える自動化された意思決定について、意味のある説明を提供できるかどうかを検証する
B. モデルのソースコードを一行ずつ確認する
C. クラウドインフラストラクチャ図の確認
D. 従業員の研修記録のみを確認する
正解: **A (**コメントを発表する**)**
説明を受ける権利（例えば、GDPR第22条に基づく権利）は、組織が個人に影響を与える自動化された決定について、有意義な情報を個人に提供できることを要求するものであり、監査人は、この機能が実際に存在し、機能しているかどうかをテストする必要がある。

質問: **5**
風力タービン発電機の故障を予測するために機械学習（ML）モデルを使用する場合、どのモデル評価指標を最優先すべきでしょうか？
A. 精度
B. 特異性
C. 精度
D. リコール
正解: **(**正解を表示します**)**
タービン故障の検出など、予知保全のユースケースでは、壊滅的な事態を防ぐために、実際の故障をできるだけ多く特定することが最も重要な課題となります。AAIA™学習ガイドでは、このような高リスクシナリオにおいては、リコールが最も適切な指標であると強調しています。なぜなら、リコールは正しく識別された真陽性の割合を測定するからです。

再現率は、陽性事例（例えば、故障）を見逃すことがコストや危険性を伴うシナリオにおいて非常に重要です。再現率が高いほど、多少の偽陽性が発生しても、実際の問題のほとんどがモデルによって検出されることが保証されます。」精度は陽性予測の正確さを、特異度は真の陰性を測定し、正確度はデータが不均衡な場合に誤解を招く可能性があります。したがって、D（再現率が最も適切です。
参考資料：ISACA Advanced in AI Audit™ (AAIA™) 学習ガイド、セクション：「AIの運用とパフォーマンス」、サブセクション：「評価指標と予測精度」

質問: **6**
IS監査担当者がAIシステムの結果をレビューする際、次のうちどれが最も大きなリスクを引き起こすでしょうか？
A. AIアルゴリズムのプロセスを文書化することの難しさ
B. AIシステムがどこに設置されているかを特定できない
C. AIシステム出力の連鎖的障害
D. システム出力の不整合がチェックされていません
正解: **(**正解を表示します**)**

質問: **7**
AIモデルのトレーニングに使用されるデータを監査する際に、最も重要な考慮事項は次のうちどれですか？
A. 代表性
B. 予測可能性
C. 適時性
D. 理解しやすさ
正解: **A (**コメントを発表する**)**

質問: **8**
再帰型ニューラルネットワークが文書の言語翻訳を可能にする最も適切な理由は次のうちどれですか？
A. プロセスは順次行われます。
B. このプロセスではアソシエーションルールを使用します。
C. この処理はグリッドデータに特化しています。
D. プロセスは一方向です。
正解: **A (**コメントを発表する**)**
リカレントニューラルネットワーク（RNN）とその派生モデル（LSTMやGRUなど）は、時系列データを処理するように設計されており、時間軸やシーケンス内の位置による依存関係を捉えます。言語翻訳では、単語やフレーズは文脈の中で解釈される必要があり、単語の意味は先行する（そして高度なアーキテクチャでは後続する）トークンに依存します。RNNは

ステップ間で内部状態を維持するため、モデルは後の出力を予測する際に、文の前半部分の情報をエンコードすることができます。
オプションB（アソシエーションルール）は、古典的なデータマイニング手法に関するものであり、RNNが翻訳に有効な根本的な理由ではありません。オプションC（グリッドデータ）は、画像処理に使用される畳み込みニューラルネットワークにより関連しています。オプションD（単方向は、本質的に利点ではありません。実際、双方向モデルが好まれることが多いです。したがって、RNNを翻訳に利用できる鍵となる特性は、逐次処理能力です。
参考文献：
ISACA、AAIA試験内容概要 - ドメイン1：AIモデル、考慮事項、および要件（AIの種類、機械学習モデル）。
ISACA、AAIAの準備で使用される一般的なAI基礎内容（自然言語処理のためのシーケンスモデル）。

質問: **9**
AIシステム開発プロセスにおいて、データ収集の際に最も重要なタスクは次のうちどれですか？
A. システムのトレーニング
B. データの層別化
C. データのクリーニング
D. システムの隔離
正解: **C** (コメントを発表する)

質問: **10**
教師ありAI学習モデルは、アルゴリズムのトレーニングに主に次のうちどれを使用しますか？
A. ランダム化データセット
B. クラスタ化されたデータセット
C. ラベル付きデータセット
D. ラベルなしデータセット
正解: (正解を表示します)

質問: **11**
AIモデルの取得およびリスク評価において、モデルカードをレビューすることの主な利点は、次のうちどれですか？
A. 文書要件への準拠
B. モデルの脆弱性とトレーニングニーズの特定
C. モデル使用に関する法的拘束力のある契約の締結
D. モデルの意図とパフォーマンスのコンテキストを理解する
正解: (正解を表示します)

「モデルカード」とは、AIモデルの意図された用途、トレーニングデータ、制限事項、およびパフォーマンス指標に関する重要な情報を提供する標準化された文書です。監査担当者やリスク管理者にとって、主な利点は「モデルの意図とパフォーマンスのコンテキストを明確に理解できる」ことです。これにより、組織はベンダーのモデルが特定のビジネス目的に適しているかどうかを判断し、導入前に潜在的なリスク（データバイアスや環境上の制約など）を特定できます。モデルカードは文書化のコンプライアンス（オプションA）をサポートする一方で、その中核的な価値は、情報に基づいた意思決定とガバナンスに必要な透明性を提供することにあります。

質問: **12**
IS監査担当者は、複雑な問題を含む監査の報告を迅速化したいと考えています。監査担当者が生成型AIを使用する最も効果的な方法は次のうちどれでしょうか？
A. 経営行動計画の最終会議で議論された行動項目を作成する
B. 詳細な調査結果と監査範囲に基づいて、エグゼクティブサマリーの草案を作成する。
C. 監査所見を正確な表現で記述し、監査結論を修正する
D. 経営陣からの新たな情報に基づき、監査の背景情報および範囲情報を修正する
正解: **(**正解を表示します**)**
AAIA™学習ガイドでは、生成型AIツールが監査の生産性を大幅に向上させる可能性があり、特にコンテンツ生成タスクにおいてその効果が顕著であると強調しています。複雑な調査結果を明確かつ簡潔な形式にまとめるエグゼクティブサマリーの作成は、生成型AIの自然言語生成機能を活用することで大きな効果が得られる、影響力の大きいユースケースです。
「生成型AIは、監査人がエグゼクティブサマリーなどのレポートセクションを自動化するために活用でき、コンテンツの明確さを損なうことなく、一貫性を確保し、時間を節約できます。」A、C、Dは有効な使用例ですが、Bは複雑な監査において時間のかかる高度なレポート作成作業を迅速化することで、最も大きな価値を提供します。
参考資料：ISACA Advanced in AI Audit™ (AAIA™) 学習ガイド、セクション：監査プロセスにおけるAI」、サブセクション：監査報告における生成型AIアプリケーション」

質問: **13**
AIシステムとデータに対する定期的な脅威モデリング演習を実施する最も重要な理由は次のうちどれですか？
A. AIシステムの潜在的な脆弱性を事前に特定する
B. AIアルゴリズムの性能を評価する
C. AI規制要件を遵守するため
D. AIモデルのドリフトの発生を防ぐ
正解: **(**正解を表示します**)**
定期的な脅威モデリングにより、組織はAI特有の脆弱性を事前に特定できます。例えば、以下のような脆弱性です。

データポイズニング
モデル反転攻撃
メンバーシップ推論攻撃
迅速な注射
モデルの不正操作
AAIAは、従来のIT脅威モデリングでは十分に対応できないAI特有のセキュリティリスクを予測し軽減するためには、AI脅威モデリングが不可欠であると強調している。

質問: **14**
規制遵守にとどまらないAIガバナンス構造を確立する最も重要な理由は、次のうちどれですか？
A. グローバルなAIデータプライバシー基準に準拠するため
B. AIシステムに対する世間の監視に伴う評判リスクを軽減するため
C. AIライフサイクル全体を通して倫理的完全性を確保する
D. AIシステムの機能を承認されたユースケースに限定するガードレールを確立する
正解: **(**正解を表示します**)**
規制遵守は不可欠ですが、AAIAは、AIの設計、展開、監視は倫理的誠実さに基づいて行われるべきであることを強調しています。規制はしばしば技術的能力に追いついていないため、コンプライアンスだけに頼ると、公平性、透明性、人間の尊厳、社会への影響といった分野でギャップが生じます。ガバナンス構造をコンプライアンスを超えて拡張する最も重要な理由は、データ収集やモデル設計から展開、監視、廃止に至るまで、AIライフサイクル（C）全体を通して倫理的誠実さを確保するためです。

質問: **15**
IS監査担当者が製造組織の在庫監査を実施しています。組織のスタッフの支援なしに、監査担当者が製品の種類を特定するのに最も適した方法は次のうちどれでしょうか？
A. 自然言語処理
B. 音声モデリング
C. ロボティック・プロセス・オートメーション（RPA）
D. コンピュータビジョン
正解: **D (**コメントを発表する**)**
コンピュータビジョンは、機械学習技術を用いて画像や動画などの視覚データを識別・分類します。在庫監査においては、人間の介入なしに製品の種類を認識したり、バーコードをスキャンしたり、保管状況を評価したりするために活用できます。
「コンピュータビジョンは、製造業のような自動化された環境において特に効果的であり、カメラやセンサーからの視覚データを処理することで、製品の識別や配置を確認することができる。」

質問: **16**

再帰型ニューラルネットワークが文書の言語翻訳を可能にする最も適切な理由は次のうちどれですか？
A. プロセスは順次行われます。
B. このプロセスではアソシエーションルールを使用します。
C. この処理はグリッドデータに特化しています。
D. プロセスは一方向です。
正解: **(**正解を表示します**)**
リカレントニューラルネットワーク（RNN）とその派生モデル（LSTMやGRUなど）は、時系列データを処理するように設計されており、時間やシーケンス内の位置による依存関係を捉えます。言語翻訳では、単語やフレーズは文脈の中で解釈される必要があり、単語の意味は先行する（そして高度なアーキテクチャでは後続する）トークンに依存します。RNNはステップ間で内部状態を維持するため、モデルは後の出力を予測する際に、文の前の部分の情報をエンコードすることができます。

有効的な**AAIA**問題集はJPNTest.com提供され、**AAIA**試験に合格することに役に立ちます！JPNTest.comは今最新**AAIA**試験問題集を提供します。JPNTest.com AAIA試験問題集はもう更新されました。ここで**AAIA**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/AAIA-mondaishu　828問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **17**
AIモデルは、車種に基づいて異なる頻度と形式で収集されたデータを使用して、車両部品の故障を予測します。このモデルのデータ入力要件を評価する際に、次のうちどれが最適な行動でしょうか？
A. モデル学習前にセンサーデータの頻度とフォーマットを標準化します。
B. センサーデータをフォーマットや頻度に関係なく単一のデータセットに統合します。
C. 前処理を簡素化するために、車種ごとに個別のモデルをトレーニングします。
D. 内部で生成されたメンテナンスログの使用を優先する。
正解: **A (**コメントを発表する**)**
信頼性の高いモデル性能と、入力データ間の有意義な比較を実現するには、データの一貫性が不可欠です。センサーデータの頻度とフォーマットを標準化することで、モデルは整合性の取れたタイムステップと一貫性のある特徴構造を受け取ることができ、偽パターン、信号の欠落、偏った予測のリスクを低減できます。これは、AAIAがAIオペレーションにおいて重視するデータ品質、データバランス、データ準備の方針と一致しています。

質問: **18**
「バイブコーディング」（高度な自然言語プロンプトに基づいてAIを使用してコードを生成する手法）を採用した組織にとって、次のうちどれが最適な推奨事項でしょうか？

A. 現在の慣行を中止してください。
B. コードレビューにセキュリティチェックリストを採用する。
C. AIに自身のコードをレビューするように促します。
D. 組織独自の暗号化システムを構築する。
正解: **B** (コメントを発表する)
「バイブコーディング」やAI支援開発には、AIが公開リポジトリ（潜在的に欠陥のあるリポジトリ）から学習した「幻覚的な」脆弱性や安全でないコーディングパターンが混入するリスクがあります。最も責任ある対策は、コードレビューのために人間が主導する厳格な「セキュリティチェックリスト」を導入することです。これにより、AIが生成したコードのすべての行が、SQLインジェクションやハードコードされた認証情報などの一般的な欠陥についてチェックされることが保証されます。AIに自身のコードをチェックさせる（オプションC）方法は、モデルがそもそもコードを作成したのと同じバイアスや論理エラーを抱えている可能性があるため、信頼性に欠けます。

質問: **19**
組織のAI手順を監査する際に、最も重要な考慮事項は次のうちどれですか？
A. セキュリティ強化のためのAIシステムアップデートの頻度
B. AIのベストプラクティスに関する従業員研修
C. AIデータ侵害発生時のバックアップと復旧
D. AIによるデータ検証とフィルタリングでデータ汚染を防止
正解: **(**正解を表示します**)**
AIシステムに入力されるデータの完全性は、極めて重要な懸念事項です。AAIA™学習ガイドでは、データポイズニング（悪意のある入力を注入することでモデルの動作を操作する攻撃）のリスクを軽減するために、検証およびフィルタリングプロセスが不可欠であることを強調しています。
「データ汚染は、AIパイプラインにおける重大な脆弱性です。効果的な対策としては、トレーニングデータソースの堅牢な検証、フィルタリング、および監視が挙げられます。これらの予防策は、モデルの信頼性とセキュリティを確保するために不可欠です。」オプションA、B、Cは重要な運用およびトレーニング対策ですが、モデルの出力と信頼性を直接損なう可能性のある技術的リスクに対処しているのはDのみです。
参考資料：ISACA Advanced in AI Audit™ (AAIA™) 学習ガイド、セクション：「AIガバナンスとリスク管理」、サブセクション：「AIデータインテグリティと攻撃防止」

質問: **20**
ある組織が皮膚がん認識モデルのトレーニングを行っています。以下の情報源から収集された写真のうち、データ整合性に関して最も大きなリスクをもたらすのはどれでしょうか？
A. がん研究のための助成金を受けている研究施設
B. オープンソースのデータ拡張ファイル

C. 世界中の画像を掲載するソーシャルメディアプラットフォーム
D. 患者の同意書に署名した皮膚科医のコホート
正解: **C** (コメントを発表する)
ソーシャルメディアプラットフォーム(C)からの画像がデータ整合性に最も大きなリスクをもたらす理由は以下のとおりです。
※画像は大幅にフィルター加工または編集されている場合があります。
* 照明、スケール、解像度に一貫性がない
* メタデータは信頼できない
* 医療診断ラベル（もしあれば）は未確認です
* 文脈が不明であり、誤った情報が含まれている可能性があります
*情報源の検証や認証はできません
AAIAは、医療AIシステムには、明確な出所、正確性、および同意を備えた、高品質で臨床的に検証済みのデータセットが必要であることを強調している。
研究施設（A）と皮膚科医のコホート（D）は、医学的に信頼性が高く、完全性の高いデータを提供する。
オープンソースの拡張ファイル（B）は合成画像であり二次的なものですが、管理されていないラベルなしのソーシャルメディア画像よりは安全です。
参考文献：
AAIAドメイン2 :データ品質、出所、正確性、およびラベルの完全性
AAIAドメイン1：高インパクトAIシステムにおけるリスク特定

質問: **21**
IS監査担当者がAIシステムの結果をレビューする際、次のうちどれが最も大きなリスクを引き起こすでしょうか？
A. AIシステムがどこに設置されているかを特定できない
B. システム出力の矛盾チェックが行われていません
C. AIシステム出力の連鎖的障害
D. AIアルゴリズムのプロセスを文書化することの難しさ
正解: **B** (コメントを発表する)
検証されていないAIの出力は、誤った結果や偏った結果が意思決定プロセスに影響を及ぼす可能性があるため、重大なリスクとなります。AAIA™学習ガイドでは、AIの出力の一貫性、正確性、妥当性を検証することは、運用者と監査者の双方にとって重要な責任であると強調しています。
監査担当者は、適切な出力検証メカニズムが整備されていることを確認しなければなりません。出力のチェックを怠ると、検出されないエラーが下流のプロセスや意思決定に影響を与える可能性が高まります。」連鎖的な障害（C）はチェックされていない出力の結果ですが、Bが根本的な問題です。AとDは物流と文書化に関するリスクをもたらしますが、直接的な影響は最も大きくありません。

参考資料：ISACA Advanced in AI Audit™ (AAIA™) 学習ガイド、セクション：監査プロセスにおけるAI」、サブセクション：AI出力の監査検証」

質問: **22**
AIソリューションの倫理的側面をレビューする際に、IS監査担当者が最も懸念すべき事項は次のうちどれでしょうか？
A. 意思決定プロセスは説明不可能です。
B. このソリューションは共有クラウド環境でホストされています。
C. モデルは最近再学習されていません。
D. ソリューションドキュメントはまだドラフト段階です。
正解: **(**正解を表示します**)**
最大の懸念は、AIシステムの意思決定プロセスが説明不可能な場合（A）、特に影響力の大きい決定や規制対象となる決定の場合です。AAIAは、説明可能性が説明責任、公平性の評価、コンプライアンス、そして国民の信頼にとって不可欠であることを強調しています。決定が説明できない場合、組織は公平性を検証したり、偏りを検出したり、規制当局や影響を受ける個人に対して結果を正当化したりすることができません。
クラウドホスティング（B）は標準的な管理方法で対応可能です。再研修の頻度（C）はパフォーマンスに影響しますが、倫理的な中核には影響しません。ドラフト文書（D）は手続き上の問題であり、倫理的な障壁ではありません。説明のつかない意思決定ロジックこそが、根本的な倫理的リスクです。
参考文献：
ISACA、AAIA試験内容概要 - ドメイン5：AIにおける倫理的および法的考慮事項（説明可能性、説明責任）。

質問: **23**
AIツールによる分析のためにデータを収集する際、IS監査担当者が最も重視すべき事項は次のうちどれですか？
A. データ分類カテゴリ
B. データの保管場所とアクセス制限
C. データ形式と構文の要件
D. AIトレーニングに使用されるモデルの重み
正解: **(**正解を表示します**)**
監査で AI ツールによる分析のためにデータを収集する場合、最も重要な即時の考慮事項は、データの形式と構文が AI ツールの要件と一致していることです (C)。正しい形式 (e.例えば、構造化されたフィールド、正しいデータ型、一貫性のある区切り文字、適切なエンコーディングなど）、AIツールが誤動作したり、データを誤って解釈したり、信頼性の低い結果を生成したりする可能性があります。AAIAの監査プロセスにおけるAIに関する領域では、AI分析を適用する前に、データの準備、クレンジング、変換を重要なステップとして強調しています。

データ分類（A）とアクセス制限（B）はセキュリティとプライバシーの観点から重要ですが、AI分析自体が正しく機能するためには、フォーマット/構文が基礎となります。モデルの重み（D）はAIのトレーニング段階に関連するものであり、監査担当者のデータ収集段階とは関係ありません。したがって、AI監査ツールに提供されるデータが適切に構造化され、構文的に互換性があることを保証することが、主要な技術的課題となります。
参考文献：
ISACA、AAIA試験内容概要 - ドメイン3：監査プロセスにおけるAI（AIベースの監査分析のためのデータ準備）。
ISACAによる、AIを活用した監査手続きにおけるデータ品質、構造、およびフォーマットに関するガイダンス。

質問: **24**
AIシステムの倫理審査を定期的に実施する最も重要な理由は次のうちどれですか？
A. システムの精度と性能を向上させるため
B. AIシステム開発を組織の価値観と原則に合致させる
C. 個人の権利の保護とシステムが整合していることを保証する
D. モデル内の潜在的なデータドリフトを特定し、軽減する
正解: **(**正解を表示します**)**
AAIATM学習ガイドは、人権を擁護し、差別的な結果を防止し、システムが公平性と合法性の範囲内で機能することを保証するためには、定期的な倫理審査が不可欠であることを強調しています。価値観との整合性（B）と逸脱の防止（D）は二次的な利点ですが、倫理上の第一の責務は個人の権利と自由の保護です。
倫理審査は、AIシステムがプライバシー、公平性、アクセス、適正手続きに関する権利を侵害しないことを保証するものです。これは、国民の信頼を築き、法的責任を回避する上で不可欠です。」オプションCは、この責任を最も明確に表現したものです。パフォーマンスと価値観との整合性は重要ですが、人間中心の安全対策を確保することに比べれば二次的なものです。

質問: **25**
以下の手法のうち、感情分析における機械学習（ML）のトレーニングを最も効果的にサポートするのはどれですか？
A. 分散分析
B. ログランク検定
C. 画像認識
D. ロジスティック回帰
正解: **(**正解を表示します**)**
感情分析とは、テキストを分類するタスクであり、テキストを（肯定的、否定的、中立的など）カテゴリに分類するものです。
ロジスティック回帰は、二値分類または多クラス分類のための基本的かつ非常に効果的な統計的手法であり、感情分析モデルの標準的な選択肢となっています。これは、入力が特定

のクラスに属する確率を推定します。Transformer (LLM) のようなより複雑なアーキテクチャが現在では一般的ですが、ロジスティック回帰は、監査の文脈において、そのシンプルさと透明性から依然としてベンチマークとなっています。画像認識と ANOVA は、感情分析に必要な言語処理には関係がなく、ログランク検定は通常、自然言語処理の分類ではなく生存分析で使用されます。

質問: **26**
ある組織が、AIベースの文書リポジトリソリューションを導入した後、既存のデータガバナンスフレームワークを見直しています。以下のうち、最も優先的に考慮すべき事項はどれでしょうか？
A. データ保持ポリシー
B. データ分類
C. データエンリッチメント
D. 定性データ収集
正解: **(**正解を表示します**)**
最も重要な考慮事項はデータ分類（B）です。なぜなら、AIベースのリポジトリは、機密情報、秘密情報、規制情報、または公開情報を含む可能性のあるさまざまな種類の文書を扱うからです。適切な分類を行うことで、アクセス制御、保持ルール、暗号化要件、およびプライバシー保護が正しく適用されることが保証されます。
データ保持（A）は重要ですが、適切な分類から派生するものです。データ拡充（C）と定性データ収集（D）は、基本的なガバナンス管理ではありません。AAIAは、堅牢なAIデータガバナンスにおける最初のステップとして分類を重視しています。
参考文献：
ISACA、AAIA試験内容概要 - ドメイン1 :プライバシーおよびデータガバナンスプログラム。

質問: **27**
モデルのハイパーパラメータ調整に最も適した手法は次のうちどれですか？
A. ベイズ最適化
B. ログランク検定
C. F1スコア分析
D. 分散分析
正解: **(**正解を表示します**)**
ハイパーパラメータチューニングとは、AIモデルの最適な設定（学習率や深度など）を見つけるプロセスです。「ベイズ最適化」は、目的関数の確率モデルを構築し、次にテストする最も有望なハイパーパラメータを選択する、効率的で自動化された手法です。単純な「グリッドサーチ」とは異なり、時間と計算コストを大幅に節約できます。F1スコア分析はチューニングの結果を測定する方法の一つですが、チューニング手法そのものではありません。

ベイズ最適化は、複雑な多次元空間において最適な構成を見つける能力があるため、高度なAI開発において好まれている。

質問: **28**
銀行組織内の顧客確認（KYC）アプリケーションにおけるAIリスクを特定する際に、IS監査人が考慮すべき最も重要な事項は次のうちどれですか？
A. 知的財産権の漏洩と無効化
B. 同業他社とのベンチマーク
C. インシデント対応計画
D. 事業の中断と経済的影響
正解: **(**正解を表示します**)**
KYC（顧客確認）のようなリスクの高い金融アプリケーションでは、AIのエラーがもたらすビジネス上および規制上の影響（例えば、顧客の誤った拒否や不正口座の検出失敗など）が最大の懸念事項となります。AAIA™学習ガイドでは、AIのリスク評価をビジネスへの影響と規制上のリスクと整合させることの重要性を強調しています。
金融機関において、AIのエラーによる最も重大なリスクは、業務の中断と規制当局からの罰金にある。
KYCモデルは、エラーがコンプライアンス違反や評判の低下につながる可能性について評価されなければならない。ベンチマーク（B）はベストプラクティスの整合性をサポートし、インシデント対応（C）は緩和策の一部であるが、Dは銀行におけるAIリスクの最も重大な結果に対処するものである。
参考資料：ISACA Advanced in AI Audit™ (AAIA™) 学習ガイド、セクション：「AIガバナンスとリスク管理」、サブセクション：「AIシステムにおけるリスク影響とビジネスとの整合性」

質問: **29**
ある組織が、回避攻撃に対して脆弱なAIベースの画像認識システムを導入しました。システムがこれらの回避攻撃を確実に軽減するために、次のうちどの方法が最も効果的でしょうか？
A. 静的ルールに基づく入力フィルタリングと検証
B. 厳格なモデル精度評価基準
C. モデルアンサンブルの実装
D. 敵対的トレーニングと定期的なバイアスレビュー
正解: **(**正解を表示します**)**
回避攻撃とは、攻撃者が入力データ（画像に微妙なノイズを加えるなど）を改変して、モデルを誤分類させる攻撃のことです。AAIATMマニュアルでは、「敵対的学習」を主要な防御策として挙げており、これは学習段階で意図的に敵対的サンプルにモデルをさらすことで、モデルの堅牢性と回復力を向上させるものです。これにより、モデルは悪意のある入力に関連するパターンを学習することができます。

質問: **30**
AIモデルの決定の公平性を確認するために、AI監査中に信頼できる証拠を収集する最善の方法は次のとおりです。
A. システムメタデータの分析。
B. 厳選されたサンプルデータセットを使用してモデルをテストします。
C. 開発者へのインタビュー。
D. エンドユーザーとのシステムインタラクションを観察する。
正解: **(**正解を表示します**)**
厳選された代表的なサンプルデータセットを用いてAIモデルをテストすることで、監査担当者はモデルの意思決定における公平性と偏りを直接評価できます。このアプローチは、AAIATM学習ガイドに概説されているベストプラクティスに合致しており、さまざまな人口統計学的属性や入力シナリオにおけるモデルの動作を定量的に分析することを可能にします。
「公平性を評価するために、監査人は管理されたデータセットを用いて、モデルの出力が特定のグループに不均衡な影響を与えていないかどうかを評価すべきである。このような実証的な検証は、定性的な手法よりも強力な証拠を提供する。」

質問: **31**
計画段階で契約書やその他の長文文書を精査する場合、関連情報を抽出するのに最適なツールは次のうちどれでしょうか？
A. ロボティック・プロセス・オートメーション（RPA）
B. 予測分析
C. 自然言語処理
D. 自己回帰シーケンスモデル
正解: **(**正解を表示します**)**

有効的な**AAIA**問題集はJPNTest.com提供され、**AAIA**試験に合格することに役に立ちます！JPNTest.comは今最新**AAIA**試験問題集を提供します。JPNTest.com AAIA試験問題集はもう更新されました。ここで**AAIA**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/AAIA-mondaishu　**328**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **32**
ある組織は、急速に進化するAI技術の中で、効果的なAIガバナンスとリスク管理を維持しようとしています。以下のうち、最も効果的な行動方針はどれでしょうか？
A. 技術スタッフに役割に応じたAIトレーニングを提供する。
B. AIトレーニングを外部ベンダーにアウトソーシングする。
C. 上級管理職向けに包括的なAI研修を実施する。

D. 継続的なAIトレーニングをセキュリティ意識向上プログラムに統合する。
正解: **(**正解を表示します**)**
効果的なAIガバナンスとリスク管理を維持するには、組織全体で継続的な意識向上を図る必要がある。
単発の研修や役割限定の研修ではなく、継続的な研修が必要です。オプションDでは、AIに関するトピック（ガバナンス、リスク、倫理、プライバシー、セキュリティ）を、既に企業全体で定期的かつ必須の仕組みとなっている既存のセキュリティ意識向上プログラムに組み込みます。これにより、急速に進化するAI技術への継続的な適応がサポートされ、既存のガバナンスおよびリスクフレームワークにAIリスクに関する考慮事項を統合するというISACAの重点事項と整合し、あらゆるレベルのスタッフが自身の責任を理解できるようになります。
選択肢AとCは対象範囲が狭すぎ、技術スタッフまたは上級管理職のみを対象としているため、効果的ではあるものの、広範かつ持続可能なガバナンスの構築には至らない。選択肢Bは社内研修を補完できるが、アウトソーシングだけでは継続性や社内方針との整合性を確保できない。
参考文献：
ISACA、AAIA試験内容概要 - ドメイン1：AIガバナンスとリスク（AIガバナンス、AIトレーニングと意識向上、プログラム指標）。
ISACA、AI監査上級試験受験者ガイド - ガバナンス、リスク、および専門的責任に関するセクション。

質問: **33**
ある組織がAIモデルを外部パートナーと共有している。あるパートナーから、モデルの出力を通じて機密データが意図せず漏洩したとの報告があった。IS監査担当者が推奨する最善策は次のうちどれか？
A. モデルを直ちに再学習させ、プライバシー保護技術を実装してください。
B. さらなる調査を行う間、モデルの出力を匿名化された結果に限定する。
C. 共有モデルを無効にし、潜在的な侵害についてパートナーに通知します。
D. すべてのパートナーのデータパイプラインを監査して、漏洩源を特定する。
正解: **C (**コメントを発表する**)**

質問: **34**
ある組織の不正検出モデルは、初期データセットでは高い精度を達成しましたが、本番環境では性能が低下しました。複雑なニューラルネットワークをトレーニングした後、トレーニング精度は検証精度よりも大幅に高くなりました。以下のうち、最も可能性の高い原因はどれですか？
A. トレーニングデータが不足しています
B. 過学習
C. アンダーフィッティング
D. 特徴量スケーリング

正解: **B** (コメントを発表する)
深層ニューラルネットワークなどの複雑なモデルが、訓練データの一般的なパターンではなく、「ノイズ」や特定の詳細を学習してしまうと、「過学習」が発生します。過学習の明確な兆候は、訓練データのパフォーマンスと検証データ／テストデータのパフォーマンスの間に大きな乖離が生じることです。AAIATMマニュアルによると、過学習が発生するとモデルが脆弱になり、実運用環境における新しい未知のデータに対して汎化できなくなります。これを軽減するために、監査担当者は、正則化、ドロップアウト、モデルアーキテクチャの簡素化などの手法を推奨する必要があります。

質問: **35**
IS監査担当者は、トレーニング、検証、テストデータセットで使用されたレコードの合計数が、元のデータセットのレコード総数を超えていることに気づきました。監査担当者にとって最も重要な判断事項は次のうちどれですか？
A. トレーニングデータセットで十分な数のレコードが使用されたかどうか
B. トレーニング、検証、テストデータセットが正しい順序で作成されたかどうか
C. 検証データセットがトレーニングデータセットと同じ数のレコードを使用しているかどうか
D. データセット内の重複レコードの利用によりデータ漏洩が発生したかどうか
正解: **D** (コメントを発表する)

質問: **36**
ある組織の不正検出モデルは、初期データセットでは高い精度を達成しましたが、本番環境では性能が低下しました。複雑なニューラルネットワークをトレーニングした後、トレーニング精度は検証精度よりも大幅に高くなりました。以下のうち、最も可能性の高い原因はどれですか？
A. トレーニングデータが不足しています
B. 過学習
C. アンダーフィッティング
D. 特徴量スケーリング
正解: **(**正解を表示します**)**
「過学習」とは、ディープニューラルネットワークなどの複雑なモデルが、トレーニングデータの一般的な基底パターンではなく、「ノイズ」や特定の詳細を学習してしまう状態を指します。過学習の明確な指標は、トレーニング性能と検証/テスト性能の間に大きなギャップが生じることです。AAIA™マニュアルによると、この状態になるとモデルは脆弱になり、本番環境における新しい未知のデータに対して一般化できなくなります。これを軽減するために、監査担当者は、正則化、ドロップアウト、モデルアーキテクチャの簡素化などの手法を推奨する必要があります。一方、過小学習（オプションC）は、両方のデータセットで性能が低下する結果となります。

質問: **37**

レンタカー会社が、需要、場所、顧客プロファイルに基づいてレンタル料金を動的に調整するAIシステムを開発しています。開発中に特定のテストを実施する最も重要な理由は次のうちどれですか？
A. モデルの価格設定ロジックがビジネス戦略と整合していることを確認するため
B. システムが既存の予約プラットフォームとシームレスに統合されるようにするため
C. AIシステムが大量の顧客からの問い合わせに対応できることを確認する
D. 価格決定が差別的な結果をもたらさないことを検証する
正解: **D** (コメントを発表する)
動的価格設定アルゴリズムは、偏ったデータや不適切な機能設計に基づいて学習された場合、意図せず保護対象グループを差別する可能性があります。AAIAは、顧客に金銭的または社会的影響を与えるあらゆるAIソリューションにおいて、公平性テストを必須要件として強調しています。
以下の点を確実にするためには、具体的な倫理的テストが必要である。
* 価格は人口統計に基づいて不当に変動することはありません
* 機密性の高い属性（民族 年齢、性別）は推測したり悪用したりしない。
顧客セグメンテーションは、保護対象グループに不均衡な不利益をもたらさない。
過去の偏りは自動価格設定には反映されない
オプションA、B、Cは重要な開発課題ではあるが、最もリスクの高い領域である差別価格設定の防止には対応していない。公平性の評価は、AAIAの重要な要件である。
参考文献：
AAIAドメイン5：倫理的なAI、公平性、差別テスト
AAIAドメイン1：AIガバナンスと影響評価

質問: **38**
IS監査担当者が、AIモデルの出力がレビューされていないことを発見しました。このリスクに最も適切に対処できるのは次のうちどれでしょうか？
A. より大きなトレーニングデータセット
B. AIの意思決定に対する検証プロセス
C. 定期的なAIモデルの再学習
D. プロンプトテンプレート
正解: **(**正解を表示します**)**
AIの出力がレビューされていない場合、主な懸念事項は、不正確、偏向的、または法令違反の決定が見過ごされる可能性があることです。このリスクに対処する最善の方法は、AIの決定に対する検証プロセス（B）を導入することです。このプロセスには、人間によるチェック、サンプリングに基づくレビュー、エスカレーション基準、および正式な承認ワークフローが含まれる場合があります。AAIAは、特に決定が財務、法律、または安全に影響を与える場合、AIの出力の監視と検証の重要性を強調しています。

質問: **39**

医療機関がデータクラスタリングを用いて、患者の病歴に基づいてグループ分けを行い、個別の治療推奨を行っています。この手法に伴う最大のプライバシーリスクは次のうちどれでしょうか？
A. クラスタリングにはより多くのデータが必要となるため、プライバシー侵害のリスクが高まります。
B. クラスタリングはモデルの複雑さを増大させ、データの匿名化を困難にする。
C. データ内の無関係な特徴は、不正確または偏った治療につながる可能性があります。
D. クラスターは、情報の提示方法によっては、機密性の高い個人情報を明らかにする可能性があります。
正解: **(**正解を表示します**)**
クラスタリング、特に医療などの機密性の高い分野では、結果として得られるグループが細分化されすぎたり、潜在的な健康状態を明らかにしたりすると、意図せず機密性の高い患者データが漏洩する可能性があります。AAIATM学習ガイドは、クラスタリングによって、個人を効果的に再識別したり、機密性の高い特性を明らかにしたりするような、小規模で均質なグループが形成されると、プライバシーのリスクが高まる可能性があると警告しています。
「クラスタリングの結果は、間接的な再識別や機密性の高い特性の意図しない暴露を防ぐために、慎重に検討されなければならない。集計された患者データの倫理的な取り扱いは、個人のプライバシーを保護するために不可欠である。」

質問: **40**
ある組織が、求職者の選考にAI採用プラットフォームを導入しました。情報システム監査担当者は、このプラットフォームの判断がモデルのバイアスによって影響を受ける可能性があることを指摘しました。監査担当者が推奨するリスク軽減策として最適なのは、次のうちどれでしょうか？
A. AIシステムのバイアスを定期的にテストし、必要に応じてパラメータを調整するプロセスを実装します。
B. トレーニングデータが公平性とコンプライアンスを検証できるまで、AIシステムの使用を一時停止する。
C. 包括性と公平性が認証された外部データセットを使用して、AIモデルを再学習します。
D. 採用が確定する前に、AI が生成したすべての採用決定について手動によるレビューを義務付ける。
正解: **(**正解を表示します**)**
バイアスに関する定期的なテストとモニタリングは、AAIA™学習ガイドに概説されているベストプラクティスに沿った、持続可能で積極的な戦略です。このアプローチにより、データや採用条件が変化しても、AIシステムが長期にわたってコンプライアンスを維持することが保証されます。
「継続的な公平性評価は、新たなバイアスを検出し、AIモデルが公平な意思決定基準を維持することを保証するのに役立ちます。定期的なテストにより、組織は規制違反や評判の低

下が発生する前に是正措置を講じることができます。」システムの停止（B）または外部データセットのみへの依存（C）は、一時的な措置または範囲が限定的な措置です。
手動レビュー（D）は効果的ではあるものの、根本的な問題を解決するものではありません。したがって、Aは包括的で監査基準に沿ったソリューションを提供します。
参考資料：ISACA Advanced in AI Audit™ (AAIA™) 学習ガイド、セクション：「AIにおける倫理的および法的考慮事項」、サブセクション：「バイアスの軽減と監視」

質問: **41**
金融機関の取引処理システムの監査を実施するためのサンプルを選択する際に、AIツールを使用する際に優先的に考慮すべき事項は次のうちどれですか？
A. サンプリングプロセスの透明性
B. 大量のデータを処理する能力
C. サンプル生成速度
D. 過去の監査における実績
正解: **(**正解を表示します**)**
監査においては、サンプリングの透明性が、サンプルが公平かつ偏りがなく、監査目的に合致していることを示すために不可欠です。AIツールが金融取引のテスト用サンプルを選択する場合、監査人は、特に経営陣、規制当局、および外部の利害関係者に対して、サンプルがどのように生成されたかを説明し、擁護できなければなりません。オプションAは、AAIAが重視する監査計画、サンプリング手法、およびAI監査証拠を直接的にサポートします。
高いスループット（オプションB）とスピード（オプションC）は有益ですが、方法論の妥当性と説明可能性に比べれば二次的なものです。オプションD（過去の実績）は役立つ場合もありますが、現在の透明性や新たな状況における適切性を保証するものではありません。AIを活用したサンプリングにおいては、選択ロジックが理解しやすく、文書化され、再現可能であることが最優先事項であり、監査の正当性を確保する必要があります。
参考文献：
ISACA、AAIA試験内容概要 - ドメイン3：AI監査ツールとテクニック（監査テストとサンプリング方法論、監査証拠収集テクニック）。
ISACAによる、AI支援監査手続きにおけるサンプリングと透明性に関する監査ガイダンス。

質問: **42**
ある組織は、AIを活用したツールを使用して、サイバーセキュリティの脅威をリアルタイムで検知し、対応しています。情報システム監査担当者は、このツールが誤検知を過剰に発生させ、セキュリティチームの作業負荷を増大させていることを発見しました。この問題に対処する上で、ツールの有効性を評価するために、監査担当者は以下のどの手法を推奨すべきでしょうか？
A. ログ分析ツールを使用して、生成されたアラートの種類と頻度を調べます。
B. システムの警告機能を業界標準と比較するためのベンチマークツールを導入する。
C. 侵入テストを実施して、システムが実際の脅威を検出する能力を評価します。

D. 機械学習（ML）検証ツールを導入して、モデルの精度とパフォーマンスを向上させます。
正解: **(**正解を表示します**)**
AAIATM学習ガイドでは、特に誤検出率が高く運用効率が損なわれる場合には、検証ツールを使用して機械学習モデルを微調整および評価することを推奨しています。機械学習の検証により、閾値の調整、再学習の必要性、または過剰なアラートの原因となっている特徴量の重み付けの誤りなどを特定できます。
「モデル検証により、組織はパフォーマンスを定量化し、誤報を減らし、運用上のニーズや脅威の状況に合わせてAIの動作を再調整することが可能になります。」

質問: **43**
ある組織が、顧客サポートのために生成型AIシステムを導入しました。このシステムでは、導入後もAIモデルが頻繁に更新されます。以下のうち、最も大きなリスクとなるのはどれですか？
A. AIに特化した変更管理ポリシーの欠如
B. AIモデルの出力に対する手動レビューへの過度の依存
C. モデル変更の継続的な監視の欠如
D. 専用のAIガバナンス委員会の欠如
正解: **C (**コメントを発表する**)**
AIモデルが本番環境で頻繁に更新される場合、パフォーマンスの低下、バイアスのずれ、誤動作、および新バージョンによって生じるセキュリティ上の問題を検出するには、継続的な監視が不可欠です。継続的な監視が行われない場合（オプションC）、組織は頻繁な変更にもかかわらず、有害な動作やコンプライアンス違反を迅速に検出できず、運用リスク、評判リスク、および規制リスクにさらされる可能性があります。
オプションA（AI固有の変更管理がない）は深刻な問題ですが、効果的なモニタリングによって問題が迅速に発見されれば、ある程度軽減できます。オプションB（手動レビューへの過度の依存）は非効率的ですが、それでも管理策としては機能します。オプションD（AIガバナンス委員会がない）は構造的な弱点ですが、モデルの変更が常に監視されていない場合、運用上のリスクが最も高くなります。AAIAはAIソリューションの監督と出力および影響のモニタリングを重視しており、継続的なモニタリングがないとこれらが直接的に損なわれます。
参考文献：
ISACA、AAIA試験内容概要 - ドメイン2：AI運用（AIソリューションの監督、AIに特化した変更管理）。
ISACAが提供する、AIシステムの継続的な監視と導入後の監督に関する資料。

質問: **44**
ランサムウェア対策にAIを統合することによる最大のメリットは次のうちどれですか？
A. 脅威インテリジェンス分析の機密保持
B. 大量のデータを分析して異常検出を強化する

C. 攻撃の責任者をより迅速に特定できるようにする
D. 従来のサイバーセキュリティ対策に必要なリソースの削減
正解: **(**正解を表示します**)**
ランサムウェアは、データアクセスや暗号化活動において、しばしば微妙で異常なパターンを伴います。AIの主な利点は、「大量のデータをリアルタイムで分析」し、従来のシグネチャベースのセキュリティツールでは見逃してしまうような行動異常を特定できることです。AIは、
悪意のある行為（ファイル名の高速変更や不正な暗号化など）の意図を認識することで、「ゼロデイ」ランサムウェアを検知します。この事前検知は、データ漏洩やシステム全体のロックアウトが発生する前に攻撃を阻止するために不可欠です。

質問: **45**
再帰型ニューラルネットワークが文書の言語翻訳を可能にする最も適切な理由は次のうちどれですか？
A. プロセスは順次行われます。
B. このプロセスではアソシエーションルールを使用します。
C. この処理はグリッドデータに特化しています。
D. プロセスは一方向です。
正解: **(**正解を表示します**)**
リカレントニューラルネットワーク（RNN）とその派生モデル（LSTMやGRUなど）は、時系列データを処理するように設計されており、時間軸やシーケンス内の位置による依存関係を捉えます。言語翻訳では、単語やフレーズは文脈の中で解釈される必要があり、単語の意味は先行する（そして高度なアーキテクチャでは後続する）トークンに依存します。RNNはステップ間で内部状態を維持するため、モデルは後の出力を予測する際に、文の前半部分の情報をエンコードすることができます。
オプションB（アソシエーションルール）は、古典的なデータマイニング手法に関するものであり、RNNが翻訳に有効な根本的な理由とは関係ありません。オプションC（グリッドデータ）は、画像処理に使用される畳み込みニューラルネットワークにより関連性の高いものです。
オプションD（一方向）は必ずしも有利なわけではなく、実際には双方向モデルの方が好まれることが多い。
したがって、RNNを翻訳に利用することを可能にする重要な特性は、逐次処理能力である。
参考文献：
ISACA、AAIA試験内容概要 - ドメイン1：AIモデル、考慮事項、および要件（AIの種類、機械学習モデル）。
ISACA、AAIAの準備で使用される一般的なAI基礎内容（自然言語処理のためのシーケンスモデル）。

質問: **46**

脅威検出に使用される生成型AIツールが不正確または誤解を招く情報を生成した場合、以下のうちどれが最も大きなリスクとなるか？
A. 組織システムに対する潜在的な脅威が見過ごされる可能性があります。
B. AI関連の主要リスク指標（KRI）の値は信頼性が低下する可能性があります。
C. 迅速な注入攻撃が成功する可能性が高くなる。
D. このモデルは脅威や脆弱性の深刻度を誇張している可能性があります。
正解: **(**正解を表示します**)**
サイバーセキュリティと脅威検出の文脈では、AI出力の「正確さ」は組織の安全性の問題です。不正確な情報（偽陰性など）の最大の危険は、
「潜在的な脅威が見過ごされる可能性がある」ため、未検出の侵害やシステム障害につながる可能性がある。
これは、モデルが真の異常を疑わしいものとして検出できない場合に発生します。

有効的な**AAIA**問題集はJPNTest.com提供され、**AAIA**試験に合格することに役に立ちます！JPNTest.comは今最新**AAIA**試験問題集を提供します。JPNTest.com AAIA試験問題集はもう更新されました。ここで**AAIA**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/AAIA-mondaishu　**328**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **47**
保険会社が保険料率を設定するためにAIモデルを使用しています。公平性に関するAI関連のポリシーに沿うために、最初にとるべき行動は次のうちどれですか？
A. 代替AIモデルをトレーニングし、バイアスを主要モデルと比較する
B. AIモデルのトレーニングデータをレビューして、潜在的なバイアスを特定する
C. 潜在的なバイアスに対処するため、AIモデルのトレーニングデータセットを修正する
D. AIモデルが提示したプレミアム料金について、顧客が異議を申し立てられるようにする
正解: **B (**コメントを発表する**)**
AAIAのガイダンスでは、公平性の評価はトレーニングデータから始めるべきだと述べている。なぜなら、バイアスはデータの選択、サンプリングの不均衡、ラベル付けの不整合、またはソースデータに埋め込まれた過去の差別によって最も一般的に生じるからである。
したがって、最初の行動方針は、トレーニングデータ（オプションB）をレビューして以下を特定することです。
偏った人口分布
欠落している、または過小評価されている集団
機密属性の不適切な使用
ラベルが間違っているか、変数が正しくエンコードされていない
差別を助長する可能性のある歴史的な決定

質問: **48**
データの適切性とバイアスという観点から、信用スコアリングシステムで使用されるAIモデルをレビューする際に、以下のうちどれを最も懸念すべきでしょうか？
A. このモデルは、過去の信用データを利用して将来の信用行動を予測します。
B. このモデルは、申請者のローン履歴を組み込んで支出習慣を評価します。
C. このモデルでは、申請者の収入レベルを信用判断の重要な要素として考慮します。
D. このモデルでは、郵便番号を信用度を判断する主要な要素として使用します。
正解: **(**正解を表示します**)**

質問: **49**
ある組織が、顧客が好みを入力すると最適な商品を提案するAIチャットシステムを導入しました。システムが顧客を不快にさせる可能性のある提案を行うリスクを軽減するための最善の方法は次のうちどれですか？
A. データセットが公平かつ偏りのないものとなるよう、トレーニングデータの量を増やします。
B. さまざまなシナリオでテストを実施し、出力が許容範囲内であることを確認します。
C. AIサーバーの継続的な監視を実施し、技術的なパフォーマンスの異常を検出します。
D. 未知のリスクを特定するために脅威分析を実施する。
正解: **(**正解を表示します**)**
ここで述べられているリスクは、顧客向けの提案が不適切、無神経、または不快なものになる可能性があるということです。最善の対策は、さまざまなシナリオ（オプションB）――エッジケース、人口統計学的変動、およびデリケートな状況――をテストし、出力が許容可能なビジネス、倫理、および顧客体験の基準内に収まっていることを確認することです。AAIAは、特に推奨事項が顧客とのやり取りに直接影響を与える場合、シナリオベースのテストと公平性／影響評価を重要な実践として強調しています。

質問: **50**
ある組織が、自社の月次データに基づいて学習させたAIモデルを開発しました。データドリフトを回避するための最適な検証方法は次のうちどれでしょうか？
A. 10分割交差検証
B. 顧客IDでグループ化して分割
C. 時系列
D. 全月にわたってランダムに分割
正解: **(**正解を表示します**)**
月次データや時系列データを扱う場合、標準的なランダム分割（オプションD）や交差検証（オプションA）では、「時間的リーク」が発生する可能性があり、これはモデルが意図せず将来のデータから学習して過去を予測してしまう現象です。
ISACA AAIA™の原則によれば、「時系列」検証は、時系列データに対して最も適切な方法です。これは、特定の期間（例1:〜10ヶ月）でモデルを学習させ、次の期間（例1:1ヶ月）でテスト

するというものです。このアプローチは、モデルが本番環境でどのように動作するかを正確に反映し、季節的な傾向や顧客行動の長期的な変化によってモデルの精度が時間とともに低下する時期を特定できるため、データドリフトの検出に不可欠です。

質問: **51**
脅威検出に使用される生成型AIツールが不正確または誤解を招く情報を生成した場合、以下のうちどれが最も大きなリスクとなるか？
A. 組織システムに対する潜在的な脅威が見過ごされる可能性があります。
B. AI関連の主要リスク指標（KRI）の値は信頼性が低下する可能性があります。
C. 迅速な注入攻撃が成功する可能性が高くなる。
D. このモデルは脅威や脆弱性の深刻度を誇張している可能性があります。
正解: **A** (コメントを発表する)
サイバーセキュリティと脅威検出の文脈において、AI出力の「精度」は組織の安全性に関わる問題です。不正確な情報（偽陰性など）による最大のリスクは、「潜在的な脅威が見落とされる」ことであり、結果として侵害やシステム障害が未検出のまま放置される可能性があります。これは、モデルが真の異常を疑わしいものとしてフラグ付けできない場合に発生します。信頼性の低いKRI（オプションB）や誇張（オプションD）は運用上の不便をもたらしますが、見逃された実際の脅威ほど壊滅的な可能性はありません。AAIA™マニュアルでは、リスクの高いセキュリティシステムにおいては、このリスクを軽減するために、出力の検証と人間の監視が必須であることを強調しています。

質問: **52**
IS監査担当者が、財務承認を自動化するAI駆動型プロセスをレビューしています。職務分掌（SOD）の維持において、次のうちどれが最大の課題となりますか？
A. AIアルゴリズムの透明性の欠如
B. 対象を絞ったAI意識向上トレーニング
C. AIツールのドキュメントが不十分
D. AIを活用して定型的な手作業を自動化する
正解: (正解を表示します)
職務分掌（SOD）は、取引の全段階を単一の人物（または組織）が管理できないようにすることで、エラーや不正を防止することを目的としています。AIが財務承認を自動化する場合、「アルゴリズムの透明性の欠如」が課題となります。なぜなら、承認を与えるロジックが不透明な場合が多いからです。アルゴリズムが「ブラックボックス」として機能すると、これまで複数の人間の役割に分散していた意思決定権限が、意思決定のプロセスを十分に把握できないまま一元化されてしまう可能性があります。その結果、不正な承認や誤った承認が見過ごされてしまう恐れがあります。効果的なAIガバナンスでは、自動化された承認が透明性のある監査証跡と二次的な人的レビューの対象となるようにし、SODの原則を遵守する必要があります。

質問: **53**
IS監査担当者が、保険料と加入資格の決定に使用されるAIモデルのテストを行っています。アルゴリズムの出力におけるバイアスを特定するために、次のうち最も効果的なテスト方法はどれですか？
A. 回帰テスト
B. クラスター間分析
C. 不均衡影響分析
D. 予測分析
正解: **(**正解を表示します**)**
不均衡影響分析は、モデルの決定が特定の保護対象グループや敏感なグループ（性別、年齢、民族、その他の属性など）に不均衡な不利益をもたらしているかどうかを検出するために使用される特定の手法です。保険料と加入資格を決定するAIモデルにとって、公平性と非差別は重要な規制上および倫理上の要件であり、AAIAの内容は、公平性とバイアス評価をAIガバナンスとリスク管理の中核要素として強調しています。
回帰テスト（A）は、変更によって以前正常に機能していたコンポーネントに欠陥が生じていないことを確認するものであり、公平性を保証するものではありません。クラスター間分析（B）はパターンを明らかにする可能性がありますが、本質的に公平性テストではありません。予測分析（D）は将来を見据えた分析を指す広い用語であり、バイアスを検出するために特別に設計された手法ではありません。
したがって、不均衡影響分析は、保険AIモデルの出力における偏りを特定するための最も適切かつ的を絞った方法である。
参考文献：
ISACA、AAIA試験内容概要 - ドメイン1：AIガバナンスとリスク（バイアス、公平性、透明性に関する考慮事項）。
ISACAのAI倫理および公平性に関するガイドラインは、AAIAの研修資料で使用されています。

質問: **54**
AIトレーニングデータのバイアステストが完了した後、テストの有効性を検証するために最も重要なチェック項目は次のうちどれですか？
A. データ検証に関するフィードバックは、主要な関係者から得られます。
B. AI出力による影響は許容リスクレベル内にとどまる。
C. AIプロセスは、期待されるサービス処理時間を満たします。
D. ユーザーの機密情報は入力前に安全にマスキングされます
正解: **(**正解を表示します**)**
組織は、バイアスを特定し軽減した後でも、AIの出力が許容できないリスクを生み出さないことを保証しなければならない。
AAIAは、偏見の軽減策が以下の結果をもたらす必要があることを強調しています。
公正な結果
正当な予測

* いずれの人口統計グループに対しても不均衡な被害は発生しない
組織のリスク許容度との整合性
オプションBはこの要件を反映しており、モデルの現実世界への影響が文書化されたリスク閾値と一致することを保証します。
選択肢Aは支持的ではあるが、有効性の証明にはならない。
選択肢Cは、公平性ではなく、業績に関するものです。
選択肢Dはプライバシーに関するものであり、偏見に関するものではありません。
したがって、リスク許容度に対する出力への影響を確認することが、最も重要な検証ステップとなる。
参考文献：
AAIA ドメイン 5: 倫理的な AI、公平性の検証
AAIAドメイン1 :リスクガバナンスと閾値評価

質問: **55**
IS監査担当者が、成長目標を達成するために融資承認数を増やすようAIモデルが最適化されていたことを突き止めた。その結果、債務不履行と予想損失が増加した。この状況に最も適切に対処できる対策はどれか？
A. 開発者にモデルスコアカードの採用を義務付ける。
B. より最近のローン申請データを追加して、モデルを再学習させます。
C. モデルで使用される許容閾値を下げる。
D. モデルの報酬関数を長期的なリスク指標に合わせる。
正解: **D** (コメントを発表する)
このシナリオは「目標の不整合」を示しており、AIが長期的な安定性（リスク）を犠牲にして短期的な目標（成長）を最適化している状況を表しています。AI開発、特に強化学習や目的関数型モデルにおいては、「報酬関数」がモデルが「成功」とみなす基準を定義します。この問題を解決するには、経営陣は「モデルの報酬関数を、デフォルト率や長期的な収益性といった長期的なリスク指標に合わせる」必要があります。これにより、AIは成長とリスク許容度のバランスをとった意思決定を行うことが保証されます。

質問: **56**
食品配達サービスがAIモデルを利用する場合、どのユースケースが組織にとって倫理的なリスクをもたらすでしょうか？
A. 時間、コスト、配送距離、顧客満足度などの指標を関連付け、サービス水準が低い顧客にクーポンを発行する。
B. ドライバーの雇用継続および解雇の決定は、業界ベンチマークと比較した総労働時間あたりの配達済み注文数に基づいて行う。
C. 食品の調理および配達にかかる総時間を業界ベンチマークと比較し、各レストランの主要業績指標およびリスク指標を設定する。

D. サービス速度と食品品質に関する顧客サービス指標を用いて、顧客維持率を予測し、収益を予測する。
正解: **B** (コメントを発表する)
運転手の解雇や雇用継続といった雇用に関する意思決定にAIを用いることは、重大な倫理的リスクを伴う。文脈や人間の審査を考慮せず、業績指標のみに基づいて判断を下す場合、そのようなシステムは不当な扱いや差別につながり、透明性と適正手続きの原則に違反する可能性がある。
雇用に関する意思決定の自動化は、差別的な結果を防ぐために慎重に進める必要がある。倫理的なAIガバナンスには、雇用に影響を与える意思決定にAIが使用される場合の監視が不可欠である。」

質問: **57**
地域医療機関向けにAIツールが導入されようとしています。AIの出力結果から個人のデータが使用されたかどうかが明らかにならないことを最も確実に保証するトレーニング方法はどれですか？
A. ラベル付き患者記録を用いた教師あり学習
B. プライバシー向上のためのトレーニング中のデータ拡張
C. モデルトレーニング中に差分プライバシーを適用
D. 公衆衛生データセットを用いた転移学習
正解: (正解を表示します)
差分プライバシーは、トレーニング時またはクエリ応答時に、綿密に調整されたノイズを導入することで、特定の個人の記録がトレーニングセットに含まれているかどうかを数学的に推測することを困難にします。医療データは非常に機密性が高く、厳格なプライバシー法が適用されるデータであるため、この技術はプライバシー・バイ・デザインを直接的にサポートし、モデルの出力から会員情報が漏洩したり、個人記録が再構築されたりするリスクを低減します。
オプションAは実際の患者記録を直接使用するため、それ自体では推論リスクを軽減するものではありません。オプションB（データ拡張）はデータセットを拡張する可能性がありますが、メンバーシップ推論攻撃に対する耐性を保証するものではありません。
オプションD（公開データを用いた転移学習）は有効な手段となり得るが、微調整に個人データが使用される場合、プライバシーリスクは依然として残る。オプションCで示されているような差分プライバシーは、出力結果から特定の個人データが使用されたかどうかが明らかにならないようにするための最も適切な制御手段である。
参考文献：
ISACA、AAIA試験内容概要 - ドメイン1：プライバシーおよびデータガバナンスプログラム、ドメイン2：AIに特化したデータ管理（データ機密性、データセキュリティ）。
ISACAのプライバシー・バイ・デザインおよびAIリスク管理の概念に関するガイダンスは、AAIAに反映されている。

質問: **58**
ある組織がAIガバナンスフレームワークを導入しようとしています。最初に確立すべき事項は次のうちどれですか？
A. モデルパフォーマンスダッシュボード
B. AIシステムにおける明確な説明責任と所有権の役割
C. ベンダーリスク評価アンケート
D. インシデント対応ランブック
正解: **B** (コメントを発表する)
ガバナンスフレームワークは、AIの成果に対する責任者（事業責任者 モデル責任者、リスク責任者）を明確に定義することから始まります。明確な責任者がいなければ、監視、インシデント対応、ベンダー管理といったあらゆる業務において、意思決定の基盤が欠如してしまいます。

質問: **59**
NISTのどの出版物が、AIライフサイクル全体にわたるAI関連リスクの管理に関する自主的なフレームワークを提供していますか？
A. NIST SP 800-53
B. NIST AIリスク管理フレームワーク（AI RMF 1.0）
C. NIST SP 800-171
D. NISTサイバーセキュリティフレームワーク1.1
正解: **B** (コメントを発表する)
Explanation:NIST AI RMFは、ガバナンス、マッピング、測定、管理という機能を中心に構成されたガイダンスを提供し、組織がライフサイクル全体を通してAIリスクを特定し、軽減するのに役立ちます。

質問: **60**
AIモデルに対する敵対的テストを実施する主な目的は次のうちどれですか？
A. AIインシデント対応計画の検証
B. 主要リスク指標（KRI）の決定
C. セキュリティ意識の向上
D. 管理上のギャップの特定
正解: **D** (コメントを発表する)
敵対的テストとは、AIモデルに対する現実世界の攻撃や悪意のある入力（敵対的サンプル、ポイズニング、回避など）をシミュレートし、意図的な悪用や敵対的な状況下でシステムがどのように動作するかを特定するものです。主な目的は、モデルとその周辺プロセスにおける弱点や制御のギャップ（D）を発見することです。例えば、入力検証の不備、監視の不十分さ、敵対的入力に対する保護策の欠如などが挙げられます。

質問: **61**
AIシステムにおいて監査証跡を維持する主な目的は以下のとおりです。

A. 計算効率を測定する。
B. モデルの精度と公平性を分析する。
C. AIに関する規制基準への準拠を確保する。
D. 意思決定の透明性と追跡可能性を促進する。
正解: **(**正解を表示します**)**

有効的な**AAIA**問題集はJPNTest.com提供され、**AAIA**試験に合格することに役に立ちます！JPNTest.comは今最新**AAIA**試験問題集を提供します。JPNTest.com AAIA試験問題集はもう更新されました。ここで**AAIA**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/AAIA-mondaishu　328問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **62**
非構造化された顧客フィードバックを使用して標準化されたレポートを生成するのに最適なAIソリューションは次のうちどれですか？
A. 異常検知
B. 自然言語処理（NLP）
C. 予測分析
D. 推薦エンジン
正解: **(**正解を表示します**)**
自然言語処理（NLP）は、非構造化テキストの処理に特化した人工知能（AI）の一分野です。監査やビジネスの現場では、NLPツールを用いて大量の顧客フィードバックに対して「感情分析」や「エンティティ抽出」を行い、共通のテーマ、苦情、あるいは好ましい傾向を特定することができます。ISACA（国際監査監査協会）によると、NLPは、人間が作成した定性的なテキストを、監査人が客観的な分析に利用できる構造化された標準化レポートに変換する最適な手段です。

質問: **63**
ある組織は、急速に進化するAI技術の中で、効果的なAIガバナンスとリスク管理を維持しようとしています。以下のうち、最も効果的な行動方針はどれでしょうか？
A. 技術スタッフに役割に応じたAIトレーニングを提供する。
B. AIトレーニングを外部ベンダーにアウトソーシングする。
C. 上級管理職向けに包括的なAI研修を実施する。
D. 継続的なAIトレーニングをセキュリティ意識向上プログラムに統合する。
正解: **(**正解を表示します**)**
効果的なAIガバナンスとリスク管理を維持するには、単発的または役割限定的な研修ではなく、組織全体での継続的な意識向上が必要です。オプションDでは、AIに関するトピック（ガバナンス、リスク、倫理、プライバシー、セキュリティ）を、既に企業全体で定期的かつ必

須となっているセキュリティ意識向上プログラムに組み込みます。これにより、急速に進化するAI技術への継続的な適応が支援され、既存のガバナンスおよびリスクフレームワークにAIリスクに関する考慮事項を統合するというISACAの重点事項に合致し、あらゆるレベルのスタッフが自身の責任を理解できるようになります。

質問: **64**
AIモデルのトレーニングに使用されるデータに関連する倫理的リスクを評価する際に、最も重要な考慮事項は次のうちどれですか？
A. 多様な出力を生成する能力
B. トレーニングデータの感度と出所
C. モデル更新の頻度
D. トレーニングデータのクリーニングおよび検証方法
正解: **(**正解を表示します**)**
倫理的リスクは、使用されるデータの性質から始まります。トレーニングデータ（オプションB）の機密性と出所によって、モデルがプライバシー侵害、過去の偏見の永続化、または適切な同意なしに収集されたデータの使用といったリスクを抱えるかどうかが決まります。AAIAは、データの出所、データの機密性、および処理の合法性を、倫理的なAIの中核として位置付けている。
健康状態、民族性、性別、経済状況などの機密性の高い属性を含むトレーニングデータは、法令遵守および倫理的な影響について慎重に検討する必要があります。
オプションA（多様な出力）はパフォーマンスに関するものであり、倫理とは関係ありません。オプションC（更新頻度）はライフサイクル管理の一部であり、倫理的な調達とは関係ありません。オプションD（データクレンジング方法）は品質を保証しますが、基となるデータが不適切または違法に取得されたものである場合、倫理的リスクには対処しません。
したがって、訓練データの機密性と出所は、倫理上の主要な要素となる。
参考文献：
AAIAドメイン5：倫理原則 公平性、データ機密性に関する考慮事項。
AAIAドメイン1 :プライバシーおよびデータガバナンスプログラム。

質問: **65**
AIを用いてデジタルコンテンツを作成する組織は、知的財産権の保護において課題に直面する。
このリスクを軽減するための最善の方法は次のうちどれですか？
A. トレーニングデータと本番データを分離します。
B. 透かしを実装する。
C. 敵対的学習を適用する。
D. ファイアウォールを実装する。
正解: **(**正解を表示します**)**

AIが生成するコンテンツ（画像 テキスト、音声など）において、「ウォーターマーク」は知的財産（IP）を保護し、出所を保証するための重要な技術的制御手段です。デジタルウォーターマークは、メタデータまたはコンテンツ自体に（多くの場合目に見えない形で）埋め込むことができ、組織が作成者であることを証明し、不正な配布を追跡します。これは、法的権利の主張とブランド保護を支えます。ファイアウォールとデータ分離はシステムを保護しますが、ウォーターマークは、オンラインまたはクライアントと共有された後の出力を保護します。AIによってコンテンツ作成が容易になるにつれ、所有権を証明できる能力は、倫理的および法的保護の不可欠な要素となります。

質問: **66**
プライバシーとデータセキュリティを保護するために最も重要なAIデータガバナンス方法は次のうちどれですか？
A. AIトレーニングに外部データソースを使用する
B. AIの許容利用ポリシーの策定
C. AIモデルのパフォーマンス指標の最適化
D. 定期的なモニタリングの実施
正解: **D** (コメントを発表する)
定期的なモニタリングは、AIシステム、特に機密データや個人データを扱うシステムにおいて、プライバシーとデータセキュリティを保護するための最も重要なガバナンスメカニズムです。ISACAのAAIAガイダンスでは、AIシステムは進化し、データドリフトが発生し、リスクエクスポージャーが変化し、プライバシーの脅威が時間とともに増加するため、データガバナンスは継続的でなければならないと強調しています。
定期的なモニタリングにより、以下のことが保証されます。
不正アクセスの検出
異常なデータ使用の特定
プライバシー管理が引き続き有効であることを確認する
データ分類ミスや漏洩の早期発見
保持、削除、最小化の要件への準拠の検証

質問: **67**
AIベースの意思決定システムを監査する際に、最も大きな課題となるのは次のうちどれですか？
A. 決定論的AIモデルの結果を考慮する
B. 逐次アルゴリズム規則の説明
C. AIモデルの透明性を理解する
D. 大規模データセットの管理
正解: (正解を表示します)
多くの最新のAIシステム、特にディープニューラルネットワークは「ブラックボックス」的な性質を持つため、意思決定がどのように行われたかを正確に理解することは困難です。AAIATMマニュアルでは、「AIモデルの透明性（および説明可能性）を理解すること」が最

大の監査課題であると指摘されています。これは、監査人が公平性を検証したり、隠れた偏見を検出したり、論理に基づく規制への準拠を確認したりする能力が制限されるためです。

質問: **68**
AIモデルの劣化リスクを軽減するための最適なアプローチは次のうちどれですか？
A. モデルがモデル生成データと人間生成データの両方で学習されていることを確認する
B. 敵対的入力を特定するための継続的な監視の導入
C. モデル学習目的で合成データの使用を増やす
D. モデルの出力と推奨事項に対する定期的な人的レビューの実施
正解: **(**正解を表示します**)**
「モデル劣化」またはモデル崩壊）とは、前回の学習以降に現実世界の環境が変化したために、モデルのパフォーマンスが徐々に悪化する現象です。最も効果的な対策は「定期的な人間によるレビュー」です。人間は、自動監視では見逃してしまう可能性のある「状況の変化」や「常識的な誤り」を特定できます。この「ヒューマン・イン・ザ・ループ」（HITL）制御により、AIの意思決定が長期にわたって根拠に基づき、正当かつ正確であり続けることが保証されます。

質問: **69**
組織がAIモデルの意思決定におけるバイアスを管理する上で、最も役立つのは次のうちどれですか？
A. 公平性基準の標準化
B. 人間の監視とフィードバックメカニズム
C. データの匿名化と分類
D. 定期的なモデル再学習
正解: **B (**コメントを発表する**)**
バイアスはしばしば微妙で文脈に依存するため、自動システムが自力で検出するのは困難です。「人間の監視とフィードバックメカニズム」（ヒューマン・イン・ザ・ループ）により、ドメインエキスパートがモデルの決定をレビューし、差別的または不公平と思われる結果にフラグを立てることができます。AAIA™フレームワークによれば、これらの人間のフィードバックループは、モデルのロジックを時間の経過とともに「修正」するために不可欠です。基準の標準化（オプションA）は良い出発点ですが、人間は機械にはない必要な「常識」と倫理的判断を提供します。人間が検証したデータなしでの再トレーニング（オプションD）は、バイアスを排除するどころか、既存のバイアスを強化するだけかもしれません。

質問: **70**
バックエンドAPIの変更後、AI搭載チャットボットが誤った金融アドバイスを提供するようになった場合、まず最初に何をすべきでしょうか？
A. チャットボットの応答速度を向上させるパッチを適用しました。

B. モデルの出力を上書きするためのルールを追加します。
C. 過去データと更新データを使用してモデルを再学習します。
D. チャットボットを一時停止し、影響を評価します。
正解: **(**正解を表示します**)**
AIシステムが誤った金融アドバイスを提供し始めた場合、まず最初に行うべきことは、継続的な被害を防ぐためにチャットボット（D）を停止することです。AAIAは、AI運用において、ユーザーを危険な意思決定から守ることを最優先事項としています。
停止措置により、組織は以下のことが可能になります。
有害なアドバイスの拡散を阻止する
* 影響を評価し、不具合のあるAPI依存関係を特定する
規制当局や顧客への損害を防ぐ
* 根本原因分析を安全に実施する
再訓練（C）は是正措置ではあるが、評価後に実施されなければならない。規則を追加する（B）ことは、より根深い問題を覆い隠してしまう危険性がある。
スピードパッチ（A）は正確性とは無関係です。
参考文献：
AAIAドメイン2：事故管理、安全管理、および出力検証

質問: **71**
AIモデルのドリフトを検出するのに最も役立つのは次のうちどれですか？
A. モデル出力の定期的な外部レビューを実施し、根本原因を特定する
B. モデル性能のベースラインを確立し、継続的なモニタリングを実施する
C. 線形回帰手法を用いてクラスター分析を実施する
D. 安定性に関するモデル精度率の評価と定性データ分析の実施
正解: **(**正解を表示します**)**
モデルのドリフトを検出するには、比較基準とリアルタイムでの可視化が必要です。AAIATMマニュアルでは、ベストプラクティスとして「パフォーマンスのベースラインを設定する」（初期検証フェーズの精度やF1スコアなどの指標を使用）こと、そして「継続的なモニタリングを実施する」ことで、モデルが実際の運用データを処理する際にこれらの指標を追跡することを推奨しています。ベースラインからの大きな逸脱は、モデルの環境が変化し、再学習が必要であることを示す早期警告となります。

質問: **72**
生成型AIシステムには、組み込みの倫理基準に照らし合わせて不適切な質問を拒否する検証制御機能が備わっている。以下のうち、悪意のある攻撃者がプロップエンジニアリングによってこの制御を回避することを可能にするものはどれか？
A. 別のAIベースのシステムによって翻訳された外国語で同じ質問を送信する
B. 質問をする理由を正当化するために理論的な状況を提示する
C. さらなる学習を経てアルゴリズムが変更された後、同じ質問を再度行う

D. メインテーマとは無関係なキーワードをランダムに配置する
正解: **B** (コメントを発表する)
迅速なエンジニアリング操作では、不適切な質問を仮説的または条件付きの形式に偽装し、AIシステムを騙してフィルターを回避させることがよくあります。AAIA™学習ガイドでは、これを生成型AIの悪用における一般的な攻撃手法として取り上げています。
「攻撃者は、倫理的制約を回避するために、AIモデルの推論パターンを悪用する目的で、クエリを学術的または理論的なシナリオとして再構成する可能性があります。監査担当者は、これらの回避手法をテストする必要があります。」その他の方法（A、C、D）は特定の条件下では有効かもしれませんが、Bが最も広く有効で、文書化されているプロンプトエンジニアリング手法です。
参考資料：ISACA Advanced in AI Audit™ (AAIA™) 学習ガイド、セクション：「AIの基礎と技術」、サブセクション：「迅速なエンジニアリングと生成型AIのリスク」

質問: **73**
ある組織が、社内のAIリスクフレームワークに基づき、新しいAIユースケースを「高リスク」に分類するかどうかを検討しています。この判断において最も重要な要素はどれでしょうか？
A. 使用されているプログラミング言語
B. 個人の権利、安全、または重要な生活機会（例：雇用、信用、医療）への潜在的な影響
C. 開発チームの規模
D. モデルをホストするクラウドプロバイダー
正解: (正解を表示します)
リスク分類フレームワーク（EU AI法のアプローチを含む）は、一般的に、AIシステムの決定が個人に及ぼす潜在的な影響に基づいてリスクを段階分けしており、技術的な実装の詳細に基づいて分類しているわけではない。

質問: **74**
監査中にAIモデルの結果の再現性を最も効果的にサポートするのは、次のうちどれですか？
A. コード、データ、モデルパラメータのバージョン管理
B. 分かりやすく書かれたユーザーマニュアル
C. 高いモデル精度
D. 大規模なトレーニングデータセット
正解: **A** (コメントを発表する)
再現性を確保するには、結果を生成するために使用された正確なコード、データスナップショット、ハイパーパラメータ、および環境を取得して再実行できることが必要です。これは、厳格なバージョン管理手法（MLOps）によって実現されます。

質問: **75**

AI監査の結果、ある融資承認モデルにおいて、特定の人口統計グループに対する拒否率が著しく高いことが判明しました。経営陣はまずどのような対応を取るべきでしょうか？
A. 監査結果をリスク許容範囲内として受け入れる。
B. 監査サンプリングが十分かどうかを判断する。
C. 包括的なバイアス分析を実施する。
D. 影響を受けた人口統計グループのデータをさらに統合する。
正解: **(**正解を表示します**)**
著しく高い拒否率は、アルゴリズムによる差別が存在する可能性を明確に示す指標である。
経営陣の第一の対応策は、公平性指標、根本原因分析、モデルの説明可能性評価、データ品質レビューを含む包括的なバイアス分析（C）を実施することである。AAIAは、公平性監査とバイアス是正をAIガバナンスの中核として優先的に位置付けている。

質問: **76**
IS監査担当者が、在庫需要を予測するAIシステムの監査を行っています。このシステムは最近、主要製品の在庫切れを予測できませんでした。以下の監査テストのうち、システムの精度を最も適切に検証できるのはどれでしょうか？
A. 入力変数に関する感度分析
B. 過去の販売データを用いた履歴テスト
C. ピーク販売期間中の負荷テスト
D. 予測アルゴリズムの単体テスト
正解: **(**正解を表示します**)**

有効的な**AAIA**問題集はJPNTest.com提供され、**AAIA**試験に合格することに役に立ちます！JPNTest.comは今最新**AAIA**試験問題集を提供します。JPNTest.com AAIA試験問題集はもう更新されました。ここで**AAIA**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/AAIA-mondaishu　**328**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **77**
AIツールによる分析のためにデータを収集する際、IS監査担当者が最も重視すべき事項は次のうちどれですか？
A. データ分類カテゴリ
B. データの保管場所とアクセス制限
C. データ形式と構文の要件
D. AIトレーニングに使用されるモデルの重み
正解: **C (**コメントを発表する**)**

監査においてAIツールによる分析のためにデータを収集する場合、最も重要な即時の考慮事項は、データ形式と構文がAIツールの要件に合致していることである（C）。
適切なフォーマット（構造化されたフィールド、正しいデータ型、一貫した区切り文字、適切なエンコーディングなど）がなければ、AIツールは誤動作したり、データを誤って解釈したり、信頼性の低い結果を生成したりする可能性があります。AAIAの監査プロセスにおけるAIに関する分野では、AI分析を適用する前に、データの準備、クレンジング、変換が重要なステップであると強調しています。

質問: **78**
ある組織が、プロモーション資料を作成するためにAI画像生成プラットフォームを使用しています。情報システム監査担当者が、そのプラットフォームのトレーニングデータに著作権で保護された画像が含まれていることを発見しました。この問題に対処するための監査担当者の最適な推奨事項は次のうちどれですか？
A. AIが生成したすべての画像にラベルを付けて、第三者のコンテンツである可能性を否定します。
B. 生成された出力に著作権で保護された画像が使用されていないことを確認するために、手動レビュープロセスを実施する。
C. トレーニングデータがクリーンアップされるまで、プラットフォームの使用を一時停止します。
D. トレーニングデータの出所とライセンスを証明するプラットフォームを使用する。
正解: **(**正解を表示します**)**
AIツールが適切なライセンスを取得し、文書化されたデータセットでトレーニングされていることを確認することは、著作権侵害や法的リスクを回避するために不可欠です。AAIA™学習ガイドでは、倫理的および法的基準を満たすために、認証済みで追跡可能なトレーニングデータを提供するプラットフォームの使用を強調しています。
組織は、AIシステムのトレーニングに使用されるデータの出所とライセンスを検証する必要があります。データソースを認証するプラットフォームは、保護された知的財産を無断で使用するリスクを軽減します。」手動レビュー（A）はリソースを大量に消費し、埋め込まれた著作権侵害を検出できない可能性があります。ラベル表示（C）は法的保護には不十分です。停止（D）は、まず是正措置を試みることなく行うには過剰である可能性があります。したがって、Bが最も戦略的かつ効果的な提案である。
参考資料：ISACA Advanced in AI Audit™ (AAIA™) 学習ガイド、セクション：「AIにおける倫理的および法的考慮事項」、サブセクション：「AIシステムにおける知的財産およびデータライセンス」

質問: **79**
攻撃者がAIシステムに問い合わせてそのロジックをリバースエンジニアリングする「モデル抽出」攻撃のリスクに最も効果的に対処できる制御策はどれですか？
A. 保存データの暗号化

B. 推論APIにおけるレート制限、クエリ監視、および出力難読化
C. モデルサイズの増加
D. 週ごとの全面的な再訓練
正解: **(**正解を表示します**)**
モデル抽出攻撃は、繰り返し行われる体系的なクエリに依存しています。APIの使用パターンに対するレート制限と異常検知は、攻撃者がモデルを再構築する能力を低下させます。

質問: **80**
販売促進活動において、AIシステムは取引履歴を分析して顧客の属性を複数のカテゴリに分類します。このプロセスの有効性を最も適切に検証するには、次のうちどれを検証すればよいでしょうか？
A. AIのパフォーマンスを安定させるために、定期的にストレステストを実施しています。
B. 適用された方法論は、ビジネス目標を適切に反映している。
C. 機密属性は入力前に他のデータ型に変換されます。
D. AIの出力のサンプリングを実施して、異常な決定を特定します。
正解: **(**正解を表示します**)**
プロモーションキャンペーンのための顧客分類など、AIを活用したビジネスプロセスの有効性は、それが定義されたビジネス目標をどれだけ適切にサポートしているかに左右されます。AAIA™学習ガイドでは、パフォーマンス監査の一環として、AI手法が意図した成果と一致していることを検証することを推奨しています。
「その有効性を測る最良の方法は、AIロジックがビジネス目標に有意義に貢献しているかどうかを評価することである。」
組織のKPIやキャンペーン戦略とのアウトプットの整合性は、機能的な成功の明確な証拠となる。オプションAとDは、運用上の回復力と品質保証をサポートする。オプションCはプライバシー保護の手法であり、有効性の検証とは直接関係がない。したがって、Bが正解である。
参考資料：ISACA Advanced in AI Audit™ (AAIA™) 学習ガイド、セクション：「監査プロセスにおけるAI」、サブセクション：「ビジネス目標とのAIの整合性の評価」

質問: **81**
以下の手法のうち、感情分析における機械学習（ML）のトレーニングを最も効果的にサポートするのはどれですか？
A. 分散分析
B. ログランク検定
C. 画像認識
D. ロジスティック回帰
正解: **(**正解を表示します**)**
感情分析は、テキストを分類するタスクです（例：肯定的、否定的、中立的）。ロジスティック回帰は、二値分類または多クラス分類のための基本的かつ非常に効果的な統計的手法であ

り、感情モデルの標準的な選択肢となっています。これは、入力が特定のクラスに属する確率を推定します。Transformer（LLM）のようなより複雑なアーキテクチャが現在では一般的ですが、ロジスティック回帰は、監査の文脈において、そのシンプルさと透明性から依然としてベンチマークとなっています。画像認識とANOVAは、感情分析に必要な言語処理とは無関係であり、ログランク検定は通常、自然言語処理の分類ではなく、生存分析で使用されます。

質問: **82**
以下のAIシステム特性のうち、IS監査担当者がシステムのアルゴリズムを評価する上で最も役立つものはどれですか？
A. AIシステムは、モデルトレーニングのための複数のオプションを提供します。
B. AIシステムアルゴリズムは、トレーニングデータを使用して意思決定の出力に反映します。
C. AIシステムは、意思決定の透明性のある根拠を提供します。
D. AIシステムは、アーカイブされた取引データを使用して意思決定を行います。
正解: **(正解を表示します)**

質問: **83**
AIモデルのトレーニングデータにクラスの不均衡が確認された場合、IS監査担当者が最も懸念すべき事項は次のうちどれでしょうか？
A. データドリフト
B. データ品質
C. バイアスモデル
D. モデルの過学習
正解: **(正解を表示します)**
クラスの不均衡は、トレーニングデータにおいて1つ以上のクラスが過小評価されている場合に発生します。最も懸念されるのはモデルバイアス（C）です。モデルが多数派クラスを優遇するように学習してしまうと、パフォーマンスが低下し、少数派クラスが不公平な扱いを受ける可能性があります。不正検出、信用スコアリング、医療診断などの重要なアプリケーションでは、これは体系的な差別や誤った判断につながる可能性があります。AAIAは、クラスの不均衡をバイアスの一般的な原因として挙げ、その軽減策（リサンプリング、重み付け、閾値調整）の重要性を強調しています。

質問: **84**
保護対象属性（例：人種）を直接使用しないモデルにおいて、代理差別をテストする最良の方法は次のうちどれですか？
A. 数値要素をすべて削除する
B. 他の相関する特徴（例：郵便番号）が、同じ異なる結果を再現する代理変数として機能するかどうかを検証する
C. モデルの正則化パラメータを増やす

D. トレーニングエポック数を減らす
正解: **B** (コメントを発表する)
代理差別は、保護対象外の特徴が保護対象の属性と強い相関関係にある場合に発生し、結果としてバイアスが再導入される。このような特徴に関する相関分析と結果分析は、これを検出するために役立つ。

質問: **85**
監査担当者が、モデルのトレーニングデータが5年前に収集されたものであり、ビジネス環境が大きく変化していることを発見しました。これは最も直接的にどのようなリスクを示唆していますか？
A. モデルの過学習
B. 概念のずれ
C. アルゴリズムバイアス
D. データ漏洩
正解: (正解を表示します)
概念ドリフトとは、入力と目標変数との間の統計的な関係が、多くの場合、現実世界の状況の変化によって時間とともに変化する現象であり、入力分布のみに関わるデータドリフトとは異なる。

質問: **86**
導入前のリスク評価において、AIモデルが組織の許容リスクを超える重大なバイアスリスクと潜在的な危害をもたらすと判断されました。次のうち、最も適切な対応はどれですか？
A. リスクを安全に管理できるようになるまで、配備を延期する。
B. モデルの学習に使用するデータを強化する。
C. 例外について取締役会の承認を得る。
D. リスク許容度を再検討し、それが適切であることを確認する。
正解: (正解を表示します)
AAIATMの学習ガイドでは、AIモデルが組織の事前定義されたリスク許容度を超えるリスクをもたらす場合（特に倫理的な危害や偏見が生じる場合）、適切な安全対策が講じられるまで導入を延期すべきであると提言しています。このアプローチにより、法的責任を回避し、ステークホルダーの信頼を維持することができます。
AIのリスクが許容範囲を超えた場合、組織は是正措置によってリスクが許容レベルまで低減されるまで、導入を一時停止しなければならない。リスク軽減策を講じずに導入を進めることは、健全なガバナンス原則に反する。」

質問: **87**
AIモデルが偏りなく動作していることを確認するために、以下のうちどれをレビューすることが最も重要ですか？
A. AIトレーニングデータ

B. AI開発環境
C. AIモデルの適応性
D. AIモデルの温度
正解: **(**正解を表示します**)**
AIモデルにおけるバイアスは、多くの場合、トレーニングデータを通じて生じます。AAIA™学習ガイドでは、公平性を確保するためには、監査担当者と開発者が、モデルのトレーニングに使用されるデータの多様性、代表性、および品質を評価する必要があると強調しています。
「AIにおけるバイアスの最大の原因は、トレーニングデータにあります。出力が特定のグループに不均衡な影響を与えたり、結果を歪めたりしないようにするためには、このデータをレビューし、監査することが不可欠です。」適応性（C）や温度（D）などのモデルパラメータは動作に影響を与えますが、ほとんどのバイアスの根本原因に対処するものではありません。開発環境（B）はインフラストラクチャをサポートしますが、倫理的保証はサポートしません。
参考資料：ISACA Advanced in AI Audit™ (AAIA™) 学習ガイド、セクション：「AIにおける倫理的および法的考慮事項」、サブセクション：「AIシステムにおけるバイアスと公平性」

質問: **88**
AIの適切な利用に関するトレーニングコンテンツをレビューする際に、以下のうちどれが最も大きなリスクとなるでしょうか？
A. この内容は、効果的なプロンプティングの使用法を網羅していません。
B. この内容は、AIの非決定論的な性質を扱っていません。
C. このコンテンツはAIモデルアーキテクチャを扱っていません。
D. コンテンツは必要なパフォーマンス指標を網羅していません。
正解: **(**正解を表示します**)**
AIの非決定論的性質とは、現代のAIシステム、特に生成AI、強化学習、確率モデルは、同一の入力が与えられた場合でも必ずしも同じ出力を生成するとは限らないという事実を指します。AAIAの倫理および運用ガイドラインによると、非決定論を理解することは、以下の点において不可欠です。
AIの挙動に対する期待値の管理
AIの出力への過度な依存を防ぐ
幻覚や矛盾した結果を特定する
人的監視体制を維持する
適切な監査証跡と説明責任のサポート
AI生成出力に対する専門家としての懐疑心を維持する
研修で非決定論について説明されない場合、従業員はAIの出力が常に権威ある、あるいは正しいと誤解する可能性があり、その結果、安全でない依存、倫理違反、監査の失敗につながる可能性がある。

質問: **89**
AIツールによる分析のためにデータを収集する際、IS監査担当者が最も重視すべき事項は次のうちどれですか？
A. データ分類カテゴリ
B. データの保管場所とアクセス制限
C. データ形式と構文の要件
D. AIトレーニングに使用されるモデルの重み
正解: **(正解を表示します)**
監査においてAIツールによる分析のためにデータを収集する際、最も重要なのは、データの形式と構文がAIツールの要件（C）に合致していることを確認することです。適切な形式（構造化されたフィールド、正しいデータ型、一貫した区切り文字、適切なエンコーディングなど）が設定されていない場合、AIツールはエラーを起こしたり、データを誤って解釈したり、信頼性の低い結果を生成したりする可能性があります。AAIAの監査プロセスにおけるAIに関する領域では、AI分析を適用する前に、データの準備、クレンジング、および変換が重要なステップであると強調しています。
データ分類（A）とアクセス制限（B）はセキュリティとプライバシーの観点から重要ですが、AI分析自体が正しく機能するためには、フォーマット／構文が基礎となります。モデルの重み（D）はAIのトレーニング段階に関連するものであり、監査担当者のデータ収集段階とは関係ありません。したがって、AI監査ツールに提供されるデータが適切に構造化され、構文的に互換性があることを保証することが、技術的な最重要課題となります。
参考文献：
ISACA、AAIA試験内容概要 - ドメイン3：監査プロセスにおけるAI（AIベースの監査分析のためのデータ準備）。
ISACAによる、AIを活用した監査手続きにおけるデータ品質、構造、およびフォーマットに関するガイダンス。

質問: **90**
提示されたモデルカードの抜粋の結論を正しく要約しているのは、次のうちどれですか？
モデルカード - 電力網の予知保全モデル
モデル情報：
* 説明：電力網コンポーネントのメンテナンスニーズを予測し、計画外のダウンタイムを削減し、電力網の信頼性を向上させるために設計されたAIモデル。
* 入力データ :リアルタイムセンサーデータ、過去のメンテナンス記録、および運用ログ。
* 出力: 60日および90日間のメンテナンスニーズ予測。評価:
* アプローチ :クロスバリデーションと、精度、適合率、再現率の検証。
* 結果：精度92%、適合率60%、再現率95%、F1スコア76%
A. AIモデルは、メンテナンスの必要性を95%の確率で正しく予測します。
B. 電力網の稼働率は72%になると予想されます。
C. 90日後に送電網の障害が発生すると予測されています。

D. F1は、モデルが真のメンテナンスの必要性を76%の確率で特定していることを示しています。
正解: **(**正解を表示します**)**
F1スコアは、精度と再現率の調和平均であり、特にクラスに不均衡がある場合（例えば、「メンテナンス不要」の結果が「メンテナンス必要」の結果より多い場合）に、モデルの精度をバランスよく示す指標となります。AAIA™学習ガイドによると、F1スコアは、偽陽性および偽陰性のリスクをバランスさせながら、モデルが真陽性をどれだけうまく識別できるかを評価するために使用されます。
「F1スコアは、モデルが関連イベント（この場合は真のメンテナンスニーズ）を正しく識別する能力を要約したものです。F1スコアが76%ということは、モデルが比較的バランスが取れており、誤ったアラートをあまり生成することなくメンテナンス要件を効果的に検出できることを意味します。」したがって、Dが正解です。オプションAは再現率を予測精度と誤って表現しています。オプションBは精度を誤って解釈しています。
選択肢Cは、抜粋箇所に直接的な根拠がない。
参考資料：ISACA Advanced in AI Audit™ (AAIA™) 学習ガイド、セクション：「AIの運用とパフォーマンス」、サブセクション：「評価指標とモデルカードの理解」

質問: **91**
金融機関における規制遵守のために使用される複雑な機械学習（ML）モデルを評価する際、情報システム監査人は透明性を最も確実に確保するために、次のうちどれを行うべきでしょうか？
A. 文書の出典とデータ処理。
B. 出力結果を表示するダッシュボードを作成する。
C. 定期的なモデル監査レポートを提供する。
D. モデルの決定を説明するツールを使用する。
正解: **D (**コメントを発表する**)**
AIにおける透明性、特に金融などの規制分野における透明性は、複雑な機械学習モデルの内部動作と出力を解釈する説明可能性ツールを用いることで最も効果的に実現できます。AAIA™学習ガイドでは、監査人と規制当局の両方が特定の決定が下された理由を理解するために、モデルの説明可能性が不可欠であることを強調しています。
「説明可能性ツールを使用すると、監査人は予測を入力機能に遡って追跡できるため、公平性、論理性、およびコンプライアンスの検証に役立ちます。これらのツールは、ブラックボックスモデルにおける透明性と信頼性をサポートします。」文書化（A）と報告（C）はガバナンスの一部ですが、Dは意思決定レベルの明確性を直接サポートします。
ダッシュボード（B）は結果を表示するものであり、根拠を示すものではない。
参考資料：ISACA Advanced in AI Audit™ (AAIA™) 学習ガイド、セクション：「監査プロセスにおけるAI」、サブセクション：「モデルの説明可能性と規制上の保証」

有効的な**AAIA**問題集はJPNTest.com提供され、**AAIA**試験に合格することに役に立ちます！JPNTest.comは今最新**AAIA**試験問題集を提供します。JPNTest.com AAIA試験問題集はもう更新されました。ここで**AAIA**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/AAIA-mondaishu　**328**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **92**
QUESTION NO: 65情報システム監査担当者が、監査を支援するために承認済みの生成型AIツールにソースデータを入力すべきかどうかを判断する
際に、最も重要な行動は次のうちどれですか？
A. ツールが最新モデルを活用していることを確認してください。
B. ツールがプライバシーに関する通知を提供していることを確認します。
C. AIモデルの幻覚が発生したかどうかを判定します。
D. 情報が信頼できるかどうかを判断する。
正解: **(**正解を表示します**)**
監査活動において生成型AIツールを使用する場合、最も重要な懸念事項は、入力および処理される情報の信頼性と適切性です。AAIATM学習ガイドによると、監査担当者は、監査データが有効かつ機密性を有し、生成された出力が事実に基づき検証可能であることを保証する責任を負います。
「情報システム監査担当者は、AIツールに入力された情報が信頼性が高く、監査の状況に適しているかどうかを評価する必要があります。機密情報や未検証のデータを入力すると、規制違反や監査の不正確さにつながる可能性があります。」

質問: **93**
ある組織が、複数のソースから大量の入力データを処理する、信用スコアリング用のニューラルネットワークベースのAIシステムを導入しました。入力データの検証と異常検知の制御が不十分な場合、次のうちどれが最大の危険となりますか？
A. 信用判断に影響を与える可能性のある偏った入力
B. 過剰な異常フィルタリングによる過学習
C. 冗長な入力チェックによる計算コストの増加
D. 過剰なデータ前処理によるモデル学習サイクルの遅延
正解: **(**正解を表示します**)**
ニューラルネットワークベースの信用スコアリングでは、モデルの複雑さによって、特定の入力と最終結果の関係が不明瞭になることがよくあります。入力検証と異常検出が弱い場合、
さまざまなソースからの「偏った入力」や「ノイズ」が、トレーニングおよび推論パイプラインに混入する可能性がある。

ISACA AIATMフレームワークによれば、こうした偏った入力によって、モデルは大規模データセットの中に隠された差別的なパターン（例えば、民族性と信用力との相関関係）を学習してしまう可能性がある。これは、非倫理的で、場合によっては違法な信用判断につながる。

質問: **94**
セキュリティの観点からAIモデルをテストする際に、最も重要なのは次のうちどれですか？
A. 回帰テスト
B. モデルの再学習
C. 脆弱性評価
D. データ検証
正解: **(**正解を表示します**)**
AIセキュリティテストでは、従来のIT脆弱性とAI特有の脅威の両方に対処する必要があります。AAIA™フレームワークによれば、「脆弱性評価」は、安全でないAPI、入力サニタイズの欠如、敵対的攻撃に対する脆弱性など、AIパイプラインの弱点を特定するために不可欠です。この評価は、システムが即時インジェクションやデータポイズニングなどの悪用に耐えられるかどうかを監査担当者が判断するのに役立ちます。回帰テスト（オプションA）は一貫性を保証し、データ検証（オプションD）は品質を保証しますが、専用の脆弱性評価は、「モデルとそのサポートインフラストラクチャのセキュリティ」状態に特化した唯一の方法です。

質問: **95**
ある組織が、AIベースの意思決定支援モデルにおける変更管理手法を評価しています。次のうち、AIに特化した効果的な変更管理を最もよく示しているのはどれですか？
A. 独立した専門家を起用し、四半期ごとにモデルの精度と正確性を検証する。
B. 責任体制を確立するために、データサイエンスチームのメンバー1名にモデルの調整を任せる。
C. トレーサビリティを確保するために、モデルの更新と再トレーニングセッションを文書化する
D. 調整ごとにモデルの別々のコピーを2つ展開して結果を比較する
正解: **C (**コメントを発表する**)**
モデルの更新と再トレーニングセッションを文書化してトレーサビリティを確保すること（オプションC）は、AIにおける成熟した監査対応可能な変更管理の特徴です。AAIATM学習ガイドには次のように記載されています。
「再学習イベント、パラメータ調整、更新理由など、すべての変更の追跡可能性と文書化は、AIシステムの効果的な監査証跡、説明責任、および規制遵守を可能にします。」レビューや比較は有用ですが、継続的な透明性と効果的な管理を保証するのは、包括的な文書化のみです。

質問: **96**
AIモデル用のデータフレームにデータを初期的に入力する際に、以下のうちどれが最も重要ですか？
A. 探索的データの分析で、誤ったデータ型、ヌル値、重複エントリをチェックします。
B. データをトレーニングデータセットとテストデータセットに分割するためのコード
C. モデルへのデータ属性の組み込み、除外、または後からの削除に関する承認済みのリスク評価
D. 相関関係や外れ値を特定する箱ひげ図、ヒストグラム、散布図、ベン図
正解: **(**正解を表示します**)**

質問: **97**
AIチームが顧客を支援するための自然言語処理（NLP）チャットボットを開発しています。収集されたデータには、非公式な会話や複数の言語が含まれています。どの前処理ステップが最も重要ですか？
A. 辞書を使って非公式な言葉遣いを標準化し、翻訳を取り入れる。
B. エンティティ認識を実行して重要な情報を抽出します。
C. トークン化とステミングを適用して複雑さを軽減します。
D. 複雑さを避けるため、英語以外のデータをすべて削除します。
正解: **(**正解を表示します**)**
自然言語処理において、学習の質は入力データの「標準化」に依存します。非公式な言語（スラング、誤字脱字）や複数の言語が混在すると、「ノイズ」が多くなり、モデルが意味を学習することが難しくなります。
辞書を用いてテキストを正規化し、翻訳サービスを用いて一貫性のあるデータセットを作成することが、最も基本的なステップです。トークン化（オプションC）と固有表現抽出（オプションB）はNLPパイプラインの標準的な要素ですが、基となるテキストが不整合であったり断片的であったりすると、効果的に機能しません。英語以外のデータを削除する（オプションD）と、多様な顧客層のニーズを満たせない、代表性のないモデルになってしまいます。

質問: **98**
生成型AIモデルにおける幻覚の最も一般的な原因は次のうちどれですか？
A. 旧型モデルカード
B. データ品質が不十分
C. アクセス制御が脆弱
D. 一貫性のない変更管理
正解: **(**正解を表示します**)**
幻覚（生成モデルが事実誤認や意味不明な情報を高い確信度で生成する事例）は、主にトレーニングセットの「不十分なデータ品質」によって引き起こされます。モデルが矛盾した

データ、不完全なデータ、または「ノイズ」（誤った事実）を含むデータでトレーニングされている場合、正確な意味関係を学習できません。ISACA AAIATM マニュアルでは、これを軽減するには、「データクリーニング」と「データ来歴」が不可欠です。

質問: **99**
IS監査担当者は、組織のインシデント管理プログラムを評価して、AI関連のインシデントを適切に管理できる体制が整っているかどうかを確認しています。監査担当者が検証すべき最も重要な項目は次のうちどれですか？
A. このプログラムでは、インシデント調査後にAIシステムを再訓練することを義務付けています。
B. このプログラムは、過去のAI関連のインシデントと解決策を利用して、現在のインシデントを分類します。
C. このプログラムには、AIモデルのドリフトやデータ整合性攻撃に対応するためのプロセスが含まれています。
D. このプログラムは、業界をリードする慣行との整合性に基づいてインシデントの優先順位を決定します。
正解: **(**正解を表示します**)**
AI関連のインシデントは、データ、モデルの動作、アルゴリズムの性能に依存するため、従来のITインシデントとは大きく異なる場合が多い。AAIATMの学習ガイドによると、インシデント管理プログラムには、モデルのドリフトの検出と軽減、データ汚染やデータ整合性攻撃からの保護など、AIに特化した機能を含める必要がある。
「AIインシデント対応フレームワークは、モデルのドリフト、敵対的入力、データ整合性侵害など、機械学習特有の問題に対応する必要があります。効果的なプログラムには、これらのAI特有の脅威に対する検出、対応、および復旧メカニズムが組み込まれています。」

質問: **100**
監査現場でAIを使用する主な利点は以下のとおりです。
A. 監査作業のレビューにおいて、担当マネージャーの時間を節約できます。
B. 大規模なデータセットをスキャンして、傾向や異常を特定できます。
C. 監査人があらゆるリスクレベルのテストプロセスを網羅するのに役立ちます。
D. 作業文書や成果物の文書化を自動化します。
正解: **(**正解を表示します**)**
AAIA™マニュアルによると、監査現場におけるAIの変革力は、データ全体の100%を大規模に処理できる能力にある。従来の監査手法は手動サンプリングに依存しており、まれな異常値や複雑な異常値を見逃す可能性があるが、AIを活用したツールは、膨大な多次元データセットを効率的にスキャンし、さらなる調査が必要な異常値や新たな傾向を特定できる。これにより、監査の深度が増し、より厳密なリスクベースのアプローチが可能になる。文書化の自動化（オプションD）や管理者の時間短縮（オプションA）は管理上の利点として有用

だが、隠れたパターンを明らかにし、監査現場の全体的な品質を向上させる分析能力に比べれば二次的なものである。

質問: **101**
AIを活用したソーシャルメディアプラットフォームは、ユーザーエンゲージメントを高めるアルゴリズムを使用していますが、意図せずして分断を招くようなコンテンツを拡散してしまう可能性があります。このリスクを軽減するための最善策は次のうちどれでしょうか？
A. ユーザーが閲覧したいコンテンツについて、ユーザーの同意を得る。
B. バイアスを減らすために、アルゴリズムを定期的に監査および調整する。
C. 懸念事項が解消されるまでアルゴリズムを一時停止します。
D. ユーザーがコンテンツの設定をカスタマイズできるコントロールを導入する。
正解: **(**正解を表示します**)**

質問: **102**
規制遵守にとどまらないAIガバナンス構造を確立する最も重要な理由は、次のうちどれですか？
A. グローバルなAIデータプライバシー基準に準拠するため
B. AIシステムに対する世間の監視に伴う評判リスクを軽減するため
C. AIライフサイクル全体を通して倫理的完全性を確保する
D. AIシステムの機能を承認されたユースケースに限定するガードレールを確立する
正解: **C (**コメントを発表する**)**
規制遵守は不可欠ですが、AAIAは、AIの設計、展開、監視は倫理的誠実さに基づいて行われるべきであることを強調しています。規制はしばしば技術的能力に追いついていないため、コンプライアンスだけに頼ると、公平性、透明性、人間の尊厳、社会への影響といった分野でギャップが生じます。ガバナンス構造をコンプライアンスを超えて拡張する最も重要な理由は、データ収集やモデル設計から展開、監視、廃止に至るまで、AIライフサイクル全体（C）にわたって倫理的誠実さを確保するためです。
選択肢Aはプライバシーのみに焦点を当てており、これはより広範な倫理的考慮事項のごく一部に過ぎません。選択肢Bも有効ですが、二次的なものです。評判の保護は、倫理的に正しいことを行った結果として得られることが多いからです。選択肢D（ガードレール）はガバナンスの一部ですが、これらのガードレールの根本的な根拠は倫理原則を遵守することです。したがって、包括的な倫理的管理こそが重要な推進力となります。
参考文献：
ISACA、AAIA試験内容概要 - ドメイン5：AIにおける倫理的および法的考慮事項（コンプライアンスを超えた倫理的AI原則）。
ISACAのAI倫理およびガバナンスに関するガイダンスは、積極的かつ価値観に基づいたAI監視を重視している。

質問: **103**

組織のAIモデル廃止プロセスを監査する際に、最も重要な考慮事項は次のうちどれですか？
A. 関連するすべてのデータ、アクセス、および依存関係が適切に廃止され、説明責任のためにポリシーに従って履歴記録が保持されていることを確認する。
B. モデルのコードリポジトリが直ちに削除されるようにする
C. 開発チームが業績ボーナスを受け取れるようにする
D. より高価な代替モデルに交換することを確実にする
正解: **A** (コメントを発表する)
適切な廃止措置には、データアクセス、依存システム、および統合の体系的な廃止が必要であり、同時に、将来の監査、調査、または規制当局からの問い合わせを支援するために十分な記録を（保持ポリシーに従って）保持する必要があります。

質問: **104**
IS監査担当者が、疑わしい取引を検出するAIベースの不正検出システムをテストしたところ、誤検出率が高いことが判明しました。検出率を最適化するために、以下のテスト方法のうちどれを優先すべきでしょうか？
A. 回帰テスト
B. 交差検証テスト
C. 実体試験
D. ベンフォードの法則の分析
正解: (正解を表示します)
交差検証テストは、モデルが独立したデータセットに対してどの程度一般化できるかを評価するために使用される統計的手法です。AAIA™学習ガイドでは、モデルの精度を微調整し、偽陽性と偽陰性の両方を減らすためのベストプラクティスとして、この手法を推奨しています。この手法では、モデルの堅牢性を確保するために、データセットをトレーニング用サブセットとテスト用サブセットに複数回分割します。
「交差検証により、監査担当者と開発者は過学習を特定し、モデルパラメータを調整して、特に不正検出の場面において、より優れた汎化性能と予測精度を実現できます。」回帰テスト（A）は時間の経過に伴う変化に焦点を当て、実証テスト（C）は監査に特化したものであり、モデルに焦点を当てたものではありません。ベンフォードの法則（D）は数値分布に適用されますが、機械学習モデルの最適化を目的としたものではありません。
したがって、Bが最良のアプローチである。
参考資料：ISACA Advanced in AI Audit™ (AAIA™) 学習ガイド、セクション：「AIの運用とパフォーマンス」、サブセクション：「テストとモデル検証方法」

質問: **105**
機械学習（ML）モデルのパフォーマンスを評価する際に、K分割交差検証を使用する主な利点は次のうちどれですか？
A. より小さなデータセットで回帰分析を実行することが容易になります。

B. 複雑なモデルを評価する際の計算コストを最小限に抑えるのに役立ちます。
C. K変数をより高い値に設定することで、モデルのバイアスを低減できます。
D. 過学習を最小限に抑えるために、複数のトレーニングとテストのサイクルを使用します。
正解: **(**正解を表示します**)**
K分割交差検証の主な利点は、複数の訓練/テスト分割を使用し、すべての分割を順番に実行することで、各観測値が異なる時点で訓練とテストの両方に使用されることです。このプロセスにより、モデルのパフォーマンスをより確実に推定でき、単一の分割への過学習のリスクが軽減されます（オプションD）。
これはモデル評価における確立されたベストプラクティスであり、AAIAが重視するAIソリューションとデータ分析のためのテスト手法とも合致しています。
オプションAは回帰分析に特化したものではなく、交差検証は分類やその他のモデルにも使用できます。オプションBは複数のモデルを学習させるため、計算コストが増加する可能性があります。オプションCはバイアス・バリアンスのトレードオフを誤解しており、Kを増やすだけでは単に「モデルのバイアスが減少する」わけではありません。重要な利点は、繰り返し多様な分割を用いることで汎化性能をより適切に評価し、過学習を防ぐことができる点にあります。
参考文献：
ISACA、AAIA試験内容概要 - ドメイン2：AI運用（AIソリューションのテスト手法、AI固有のテスト）。
ISACAのデータ分析コンテンツは、AAIAの準備において、標準的な評価方法としての相互検証を扱っています。

質問: **106**
IS監査担当者が、ベンダーからのメールに埋め込まれた「プロンプトインジェクション」を検出しました。このメールは、テキストを隠すために不可視フォントを使用していました。次のうち、最も適切な対策はどれですか？
A. 温度を下げることで、AI モデルが注射に従う可能性を低くします。
B. AIモデルに、見えないテキストを無視するように指示を追加します。
C. 取り込み前に目に見えないテキストを削除するテキストサニタイズを実装します。
D. フォントをデフォルトに変更するテキストサニタイズを実装します。
正解: **C (**コメントを発表する**)**
これは「隠しテキスト」攻撃であり、攻撃者は人間には見えないが機械が処理できる命令を埋め込むことでLLMを欺きます。最も効果的な「インシデント管理」対策は「テキストサニタイズ」であり、テキストをAIに送信する前に、目に見えない書式設定、隠しHTMLタグ、またはゼロ幅文字を具体的に削除します。

有効的な**AAIA**問題集はJPNTest.com提供され、**AAIA**試験に合格することに役に立ちます！JPNTest.comは今最新**AAIA**試験問題集を提供します。JPNTest.com AAIA試験問題集はもう更新されました。ここで**AAIA**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/AAIA-mondaishu　**328**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **107**
AIを活用した医療診断ツールは大量の患者データを必要とするため、プライバシーやデータ漏洩に関する懸念が生じます。このリスクを軽減するための最も効果的な戦略は次のうちどれですか？
A. データを暗号化し、安全なチャネルを通して送信します。
B. ツールがアクセスできるデータセットを公開されているものだけに制限する。
C. データ分析に使用するため、すべての患者からデータを収集します。
D. モデルのトレーニングには、合成データまたは匿名化されたデータセットを使用します。
正解: **D** (コメントを発表する)
患者の機密データを保護する最も効果的な戦略は、モデルのトレーニングに合成データまたは匿名化されたデータセットを使用することです。これにより、個人を特定できる情報の漏洩リスクを低減しつつ、モデルが有意義な医療パターンを学習できるようになります。
AAIAは、医療などの高リスク分野において、プライバシー・バイ・デザイン、匿名化、および個人データの生データの使用を最小限に抑えることを重視しています。匿名化と合成データは、再識別やデータ漏洩による被害のリスクを大幅に低減します。
オプションA（暗号化は転送中のデータを保護しますが、プライバシーリスクを完全に排除するものではありません。オプションBは、医療モデルに必要なのは公開データではなく臨床的に関連性の高いデータセットであるため、現実的ではありません。オプションCはデータ公開範囲を拡大し、プライバシーリスクを悪化させます。
したがって、匿名化データまたは合成データを使用することが、医療コンプライアンス原則に沿った最も強力なプライバシー保護策となる。
参考文献：
AAIAドメイン5：データプライバシー、AI倫理、およびコンプライアンス。
AAIAドメイン2：機密性の高いAIユースケースのためのデータ管理手法。

質問: **108**
生成型AIモデルの説明可能性を評価する際に、情報システム監査担当者が直面する最大の課題は次のうちどれですか？
A. モデルタイプに関する意見の相違
B. 偏ったデータの入力を防ぐことの難しさ
C. 過剰な計算によるパフォーマンスの問題

D. AIの学習が進むにつれてアルゴリズムも変化する
正解: **(**正解を表示します**)**
IS監査担当者が生成型AIモデルの説明可能性を評価する上で最大の課題は、AIが学習を続けるにつれてアルゴリズムの性質が変化することです（選択肢D）。生成型AIモデル、特に深層学習や強化学習などの高度な技術を使用するモデルは、継続的または動的な学習を採用することが多く、その結果、モデルは時間とともに進化します。このような適応性により、ロジック、パラメータ、または意思決定経路が継続的な再学習やリアルタイム学習によって変化する可能性があるため、説明可能性が著しく阻害される可能性があります。
ISACAのAdvanced in AI Audit™（AAIATM）学習ガイドでは、「継続的に学習するAIシステムは、その内部表現や推論が導入後に変化する可能性があるため、特定の時点での出力の根拠を完全に把握し説明することが困難になるなど、特有の監査上の課題を提示する」と強調しています。

質問: **109**
動物病院のIS監査担当者は、予測モデルに犬種カテゴリ変数が必要であることを知らされました。次のうち、最もリスクが高いのはどれですか？
A. データスケーリングは利用されていません。
B. クラスタリングは利用されませんでした。
C. 順序ラベルエンコーディングが使用されました。
D. ワンホットエンコーディングが使用されました。
正解: **(**正解を表示します**)**
順序尺度による符号化では、数値が順序に従って割り当てられます（例：プードル＝1、ラブラドール＝2、ハスキー＝3）。これは犬種間の階層構造や順位付けを誤って示唆し、モデルに偏りをもたらします。
AAIAは、カテゴリ変数の誤ったエンコードが以下の問題を引き起こす可能性があることを強調しています。
* 人為的に重み付けされた重要度
* 誤解を招く相関関係
* 誤った順序に基づく不正確な予測順序のないカテゴリの場合、ワンホットエンコーディング（D）が正しい低リスクのアプローチです。スケーリングの欠如（A）はカテゴリフィールドには直接関係ありません。クラスタリング（B）は無関係です。したがって、順序エンコーディングは最も高いリスクをもたらします。
参考文献：
AAIAドメイン2：データエンコーディング、特徴量エンジニアリング、およびバイアス回避。

質問: **110**
利益相反や共謀の有無を監査するために、AIを最も効果的に活用する方法は次のうちどれですか？

A. 相関行列
B. 時系列分析
C. グラフ分析
D. モンテカルロシミュレーション
正解: **(**正解を表示します**)**
「グラフ分析」またはネットワーク分析）は、「関係性リスク」を監査するための優れたAI技術である。
この手法では、エンティティ（人物、ベンダー、従業員など）を「ノード」、それらの相互作用を「エッジ」としてマッピングします。これにより、監査担当者は、標準的な表形式分析では見逃してしまうような、複数の関係者が結びついている「共謀リング」を視覚化して検出することができます。

質問: **111**
以下のテスト手法のうち、組織のデータガバナンスプログラムがAIモデルのトレーニングと展開におけるデータ品質と整合性を効果的に保証しているかどうかを最も適切に検証できるのはどれですか？
A. AIモデルの不具合による影響を評価するための事業影響分析（BIA）を実施する
B. 組織のAIソフトウェア開発ライフサイクル文書のレビュー
C. モデルの脆弱性を特定するための侵入テストを実施する
D. データソースのトレーサビリティを検証するためのデータ系統の評価
正解: **(**正解を表示します**)**
データリネージを評価することで、データのライフサイクル全体における発生源、流れ、および変換に関する洞察が得られ、これはデータガバナンスの検証に不可欠です。AAIATM学習ガイドでは、AIモデルのトレーニングに使用されるデータの正確性、一貫性、および信頼性を確保するために、データリネージが不可欠であると述べています。
「データソースのトレーサビリティは、効果的なデータガバナンスの中核をなす原則です。データリネージの検証は、データの品質を確保し、不正な改ざんを防止し、監査可能性を維持します。」

質問: **112**
動物病院のIS監査担当者は、予測モデルに犬種カテゴリ変数が必要であることを知らされました。次のうち、最もリスクが高いのはどれですか？
A. データスケーリングは利用されていません。
B. クラスタリングは利用されませんでした。
C. 順序ラベルエンコーディングが使用されました。
D. ワンホットエンコーディングが使用されました。
正解: **C (**コメントを発表する**)**
順序エンコーディングでは、数値を順序に従って割り当てます（例：プードル＝1、ラブラドール＝2、ハスキー＝3）。

これは品種間の階層構造や順位付けを誤って示唆し、モデルに偏りをもたらす。
AAIAは、カテゴリ変数の誤ったエンコードが以下の問題を引き起こす可能性があることを強調しています。
人為的に重み付けされた重要度
誤解を招く相関関係
誤った順序に基づく不正確な予測

質問: **113**
研究機関が科学データの分析に生成型AIモデルを使用しているかどうかを監査する際、幻覚的な結果を防止し、出力の正確性を確保するために、以下のうちどれを評価することが最も重要ですか？
A. データ品質の維持に役立つデータ匿名化プロセスの有効性
B. データ処理前にデータバイアスを検出・修正するように設計された生成AIモデルのアルゴリズム
C. 入力データの完全性と正確性を検証するデータ監査の頻度
D. 生成型AIモデルへの入力データの適切性と関連性を確保するために講じられている措置
正解: **(**正解を表示します**)**
入力データが適切かつ関連性のあるものであることを確認すること（オプションD）は、生成モデルが捏造されたり誤解を招くような出力を生成する幻覚を防ぐ上で最も重要な要素です。
AAIATMの学習ガイドには、「生成モデルは入力データに非常に敏感であり、不正確、無関係、または不適切な入力は、意味不明または誤った出力が発生する可能性を高めます」と記載されています。バイアス検出、データ品質監査、匿名化は重要ですが、入力データの関連性と適切性を確保することは、信頼性の高い生成AIのパフォーマンスの基盤となります。

質問: **114**
どの規制枠組みが、AIシステムのリスクを段階的に分類する（許容できない、高い、限定的、最小限）か？
A. GDPR
B. EU人工知能法
C. SOX
D. PCI DSS
正解: **(**正解を表示します**)**
EUのAI法は、AIシステムをリスクレベルに分類しており、高リスクシステムは適合性評価、文書化、および人的監視の要件の対象となる。

質問: **115**
AIシステムの導入をレビューする際に、IS監査人が考慮すべき最も重要なリスクは次のうちどれですか？
A. AIシステム保守に関連する費用

B. 業界におけるAIシステムの未成熟
C. AIシステムの意思決定におけるバイアス
D. AI技術の利用に対する抵抗
正解: **(**正解を表示します**)**
AIによる意思決定におけるバイアスは、特にAIが採用、融資、医療などの分野に影響を与える場合、最も重大なリスクの一つです。AAIATM学習ガイドでは、バイアスのあるモデルがもたらす倫理的および運用上の影響、すなわち差別、法的責任、評判の低下につながる可能性について解説しています。
AIの出力におけるバイアスは、偏った学習データや欠陥のあるアルゴリズムに起因する可能性があります。監査担当者は、バイアス検出や公平性テストなどの軽減策が実施されているかどうかを評価する必要があります。」

質問: **116**
AIを使用して監査レポートを作成する際の最大のリスクは次のうちどれですか？
A. AIシステムは、監査レポート全体で一貫性のないフォーマットを使用しています。
B. AIシステムが制御効果を誤って表示している。
C. AIシステムは管理ダッシュボードツールと統合できません。
D. AIシステムは過去の監査結果を含めることができません。
正解: **(**正解を表示します**)**
AIを用いて監査報告書を作成する際の最大のリスクは、統制の有効性（B）を誤って表現してしまう可能性があることです。例えば、統制の堅牢性を過大評価したり、欠陥を過小評価したり、調査結果を不正確に要約したりする可能性があります。これは監査全体の信頼性を損ない、不適切な経営判断、規制上の問題、そして企業の評判の低下につながる可能性があります。AAIAは、AIが生成した成果物であっても、監査の証拠と結論を正確に反映させるためには、専門家の判断と検証が必要であることを強調しています。
書式の不整合（A）と統合性の欠如（C）は、ユーザビリティと効率性の問題であり、根本的な保証リスクではありません。過去の調査結果を組み込むことができない（D）ことは、文脈を損なうものの、現在の統制評価を本質的に誤って表現するものではありません。したがって、保証の観点から最も重大なリスクは、統制の有効性の誤った表現です。
参考文献：
ISACA、AAIA試験内容概要 - ドメイン3：監査プロセスにおけるAI（監査報告とコミュニケーション）。
ISACAによる、監査における専門家としての懐疑心とAI生成による知見の検証に関するガイダンス。

質問: **117**
銀行のAI信用スコアリングシステムの監査中に、情報システム監査担当者は、申請者が自動意思決定について知らされていなかったことを発見しました。監査担当者は、まず次のうちどれを行うべきでしょうか？

A. 透明性制御を評価する。
B. 監査報告書を作成する。
C. 不服申し立て手続きを評価する。
D. 説明可能性評価を実施する。
正解: **(**正解を表示します**)**
透明性は、特にGDPRのような規制の下では、AIシステムにとって基本的な法的および倫理的要件であり、データ主体に自動意思決定について通知することが義務付けられています。監査人が申請者に通知されていなかったことを発見した場合、最初のステップは「透明性管理を評価する」ことです。これは、通知プロセスが失敗した理由を特定し、不遵守の範囲を評価するためです。これには、ユーザー契約、プライバシー通知、およびコミュニケーション手順のレビューが含まれます。失敗が理解され、リスクが評価されたら、監査人は異議申し立てプロセスの評価（オプションC）または最終レポートの作成（オプションB）に進むことができます。

質問: **118**
AIモデルが正しい予測を行う能力を持っていることを確認するために、IS監査人が最も使用する可能性が高いのは次のうちどれですか？
A. 敵対的テスト
B. グループ分析
C. レイテンシーテスト
D. 混同行列
正解: **(**正解を表示します**)**
混同行列は、機械学習およびAI監査における重要な性能評価ツールである。
AAIATMの学習ガイドによると、混同行列は実際の分類と予測された分類に関する詳細な情報を示し、監査担当者が正確性、精度、再現率、F1スコアを評価することを可能にする。「混同行列は、予測が正しかった頻度だけでなく、誤検出（偽陽性）および偽陰性）の種類も明らかにし、モデルの予測信頼性を明確に示します。」敵対的テストは堅牢性を評価し、グループ分析はサブグループ間のバイアスを特定し、レイテンシーテストは予測精度ではなくパフォーマンス速度を検証します。したがって、Dは正しい予測を保証する上で最も関連性の高い指標です。

質問: **119**
ある銀行が、顧客取引データに基づいて学習させたAIモデルをマルチクラウド環境に導入しようとしています。データセキュリティとプライバシーに関する規制遵守を最も適切にサポートするのは、次のうちどれでしょうか？
A. プライバシー・バイ・デザイン
B. データ保護影響評価（DPIA）
C. データの所在地と主権の管理
D. データガバナンスフレームワーク

正解: **C** (コメントを発表する)
マルチクラウド環境では、データはしばしば様々な地理的地域を横断します。金融機関にとって、「データの所在と主権」は最も重要なコンプライアンス要素であり、データが法律で定められた管轄区域（GDPRや各国の銀行法など）内で保存および処理されることを保証する必要があります。データの所在を管理できないと、重大な法的罰則を受ける可能性があります。「プライバシー・バイ・デザイン」や「DPIA」は不可欠な手法ですが、クラウドプロバイダー間でのデータの物理的および法的所在については具体的に規定していません。主権管理は、銀行がデータ資産に対する管理権を維持し、特定の国境を越えたデータ転送規制を遵守することを保証するものです。

質問: **120**
業務効率化のため、ある銀行は口座における不正行為を自動的に検知・防止するAIアプリケーションを導入しました。しかし、顧客からは普段行っている取引が拒否されるという懸念の声が上がっています。以下のうち、誤検知の最も可能性の高い原因はどれでしょうか？
A. データバージョン管理機能は開発されていませんでした。
B. 計算スケールのトレーニングは実施されませんでした。
C. ハイパーパラメータは最適化されていません。
D. 同意が適切に管理されていません。
正解: (正解を表示します)

質問: **121**
AIモデルのトレーニング前にデータカテゴリを変換する場合、次のシナリオのうち、最も大きなリスクとなるのはどれですか？
A. オプションの車の色を表すデータ属性をワンホットエンコーディングし、赤、青、緑、黒、白のいずれかを選択します。
B. オプションの製品フレーバーのデータ属性にダミー変数を作成し、バニラ、チョコレート、ストロベリー、バナナのオプションを設定します。
C. 顧客報酬カテゴリのデータ属性をワンホットエンコーディングし、エコノミー、ビジネス、ファーストクラスのオプションを選択します。
D. ラブラドール、テリア、ビーグルの選択肢に対して、データ属性「犬種」のダミー変数を作成する。
正解: **C** (コメントを発表する)

有効的な**AAIA**問題集はJPNTest.com提供され、**AAIA**試験に合格することに役に立ちます！JPNTest.comは今最新**AAIA**試験問題集を提供します。JPNTest.com AAIA試験問題集はもう更新されました。ここで**AAIA**問題集のテストエンジンを手に入れます。最新版

のアクセス、https://www.jpntest.com/shiken/AAIA-mondaishu　328問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **122**
AI監査ツールが、ビジネス上の意思決定に偏りがあると誤って警告を発し、不適切な経営行動計画につながった。このリスクを最も効果的に防止できるのは次のうちどれか？
A. 異なる公平性の定義を使用する。
B. 説明可能なAI検証手法を適用する。
C. オーバーサンプリングするためにグループの重みを再調整します。
D. 前提条件を文書化し、範囲を記録する。
正解: **(**正解を表示します**)**
AIツールは、データの解釈を誤ると、バイアス検出において 偽陽性」を生じる可能性があります。経営陣が誤った監査結果に基づいて行動することを防ぐため、 説明可能なAI（XAI）」検証手法（SHAPやLIMEなど）を適用する必要があります。XAIを用いることで、監査担当者は、ツールが特定の決定をバイアスありと判断した理由を理解できます。
ツールの推論に欠陥がある場合（例えば、正当なビジネス上の根拠を無視した場合）、監査人はその指摘が経営陣に伝わる前に修正することができます。これにより、AIによる監査結果に 監査人の懐疑心」と人間の検証という必要な層が加わります。

質問: **123**
特定の年のデータに基づいて学習させた、製品推奨に使用されるAIモデルの精度が、顧客の購買パターンが持続可能な製品へと変化したことにより、2年後に低下している。以下のうち、最も可能性の高い原因はどれか？
A. データドリフト
B. スキーマのずれ
C. データラベリング
D. 共変量シフト
正解: **(**正解を表示します**)**
データドリフト（モデルドリフトまたはコンセプトドリフトとも呼ばれる）とは、対象変数または入力データの統計的特性が時間とともに変化し、モデルのパフォーマンスが低下する現象を指します。このシナリオでは、顧客の嗜好が持続可能性へと根本的に変化したことが、モデルの元のトレーニングデータではもはや反映されない現実世界の環境の変化を表しています。AAIATMガイドラインに記載されているように、小売業のような動的な環境で運用されるモデルは、過去のパターンがもはや予測に役立たなくなった時期を検出するために、継続的な監視が必要です。

質問: **124**
本番環境ではまだ発生していない、影響の大きい稀なシナリオをテストする際に、IS監査担当者にとって最も役立つのは次のうちどれでしょうか？

A. 匿名化された履歴データ
B. 合成データ
C. 匿名化データ
D. ベンチマークデータセット
正解: **(**正解を表示します**)**
「エッジケース」や「稀なシナリオ」（しばしば「ブラックスワン」イベントと呼ばれる）については、過去のデータだけでは不十分です。なぜなら、それらの事象はまだ発生していないからです。「合成データ」とは、実際のデータの統計的特性を維持しつつ、稀な事象をシミュレートした人工的に生成されたデータです。これにより、監査担当者は、大規模な市場暴落や稀な医療緊急事態といった極端な状況下で、AIモデルがどのように反応するかを「ストレステスト」することができます。
匿名化または非識別化されたデータは、過去の出来事のみを反映しています。合成データを使用することは、予測不可能な環境下におけるAIの安全性と堅牢性を確保するための、積極的なテスト戦略です。

質問: **125**
監査中にAIを使用してデータ品質を評価することの最大のメリットは次のうちどれですか？
A. 規制遵守のための手続き審査の効率性
B. データ分析に関連する処理コスト
C. モデル予測に影響を与えるデータエラーを示す外れ値の特定
D. モデル予測にサンプルデータ集団を利用できる能力
正解: **(**正解を表示します**)**
従来のデータ品質チェックは、多くの場合、手動サンプリングに依存しており、まれではあるものの重大なエラーを見落とす可能性があります。AIを活用した監査ツールは、データエラー、異常、または潜在的な不正行為を示す「外れ値」を特定するために、母集団の100%を分析できます。AAIA™フレームワークによれば、これらの外れ値を特定することは非常に重要です。なぜなら、「汚れたデータ」は、AIモデルの予測と監査結論を根本的に歪める可能性があるからです。データの不整合の検出を自動化することで、監査担当者は手作業による作業を高リスク項目の調査に集中させることができ、それによって監査の精度とモデルトレーニングに使用されるデータの全体的な信頼性の両方を向上させることができます。

質問: **126**
IS監査担当者は、ウォークスルー会議の監査記録を作成するために、生成型AIを利用しています。最終版には一般的な表現が用いられ、重要な例外事項が漏れています。AI生成文書の信頼性を向上させるには、どのような対策が有効でしょうか？
A. モデルの温度設定を上げる
B. 監査証跡ログの活用と監視
C. 教師なし学習を用いた合成文書生成

D. 迅速なエンジニアリングと文脈的アンカーリングによるAIの誘導
正解: **(**正解を表示します**)**
生成型AIが一般的または「曖昧な」要約を生成する場合、多くの場合、会議の具体的なコンテキストが欠けていることが原因です。「迅速なエンジニアリングとコンテキストのアンカーリング」とは、AIに明確な指示（例：「管理例外に焦点を当てる」）を与え、要求を特定のデータ（例：「添付の会議議事録のみを参照する」）にアンカーリングすることです。ISACAによると、この手法はモデルの注意を向けさせ、幻覚や省略の可能性を低減します。「温度」を上げる（オプションA）と、実際にはモデルがよりランダムになり、信頼性が低下します。アンカーリングにより、AIは監査ウォークスルーの実際の事実に基づいたままになります。

質問: **127**
以下のうち、AIモデルが大量の非構造化データの分析を伴う複雑な問題を解決するのに最も適しているのはどれですか？
A. 強化学習（RL）
B. サポートベクターマシン（SVM）
C. 自然言語処理（NLP）
D. ディープラーニング
正解: **(**正解を表示します**)**
ディープラーニングは、多層ニューラルネットワークに基づく機械学習の一分野であり、画像、音声、複雑なテキストなどの高次元の非構造化データを処理するように設計されています。SVMなどの従来のアルゴリズムとは異なり、ディープラーニングモデルは「自動特徴抽出」を実行するため、手動によるエンジニアリングなしに関連パターンを識別できます。AAIA™マニュアルでは、ディープラーニングがコンピュータビジョンや生成モデルにおける現代のAIブレークスルーの基盤技術であると強調しています。NLP（オプションC）はディープラーニングを使用する分野ですが、「ディープラーニング」は、あらゆるドメインにわたる膨大な非構造化データセットの処理を可能にする、より広範な技術エンジンです。

質問: **128**
AI導入の文脈において、組織の変更管理プログラムにとって最も重要な行動は次のうちどれですか？
A. 組織内にAIガバナンス専門委員会を設置する
B. AIシステムの変更、更新、パッチに関するドキュメントのレビュー
C. AI関連の変更に特化した包括的なリスク評価を実施する
D. 全従業員が必須のAI倫理研修を修了していることを確認する
正解: **(**正解を表示します**)**
AAIATM学習ガイドでは、AIの実装はシステムに動的かつ非決定的な要素を導入し、変更に伴うリスクを高めることを強調しています。そのため、包括的なAI固有のリスク評価は、

アップデート、再トレーニング、またはパラメータ調整によって脆弱性や意図しない結果が生じないようにするための変更管理プログラムにおいて最も重要な要素となります。
AIに特化したリスク評価は非常に重要です。なぜなら、モデル、トレーニングデータ、インフラストラクチャの変更は、パフォーマンスや倫理遵守に影響を与えたり、システムを新たな脅威にさらしたりする可能性があるからです。標準的なIT変更レビューでは不十分な場合が多いのです。」

質問: **129**
以下のAI関連文書のうち、IS監査担当者がハイパーパラメータチューニング記録を評価する際に役立つものはどれですか？
A. データシート
B. モデル開発ログ
C. 説明可能性レポート
D. リスク評価報告書
正解: **(**正解を表示します**)**
ハイパーパラメータチューニングとは、学習率、バッチサイズ、レイヤーの深さなどの設定を調整してパフォーマンスを最適化することです。このプロセスは「モデル開発ログ」に記録され、データサイエンティストが実行したさまざまな「実験」、それぞれの実験で使用されたパラメータ、および結果として得られたパフォーマンス指標（精度や損失など）が記録されます。監査担当者にとって、これらのログはモデル構築の「監査証跡」となります。データシート（オプションA）はデータセットに関する高レベルの情報を提供し、説明可能性レポート（オプションC）は出力に焦点を当てていますが、開発ログはモデルが最終状態に「チューニング」された技術的な履歴を提供します。

質問: **130**
AIベースのマーケティング分析ツールが5年前のデータで学習されている場合、次のうちどれが最も起こりやすいでしょうか？
A. モデル抽出
B. モデル中毒
C. モデル反転
D. モデルドリフト
正解: **D (**コメントを発表する**)**
モデルドリフト（概念ドリフトとも呼ばれる）は、トレーニングに使用されるデータが現在の環境を反映しなくなった場合に発生します。マーケティングにおいては、消費者の行動、トレンド、人口統計は急速に変化するため、5年前のデータでトレーニングされたモデルは深刻なドリフトに見舞われます。AAIATMのマニュアルでは、この結果、モデルが時代遅れのパターンに基づいて予測を行うようになり、精度が低下し、偏った、あるいは無関係なマーケティング推奨事項につながる可能性があると説明されています。

質問: **131**
組織がユーザーの明示的な同意を得ずに、公開されているソーシャルメディアデータを使用してAIモデルをトレーニングする場合、以下のうちどれが最大の危険となるでしょうか？
A. 不正確で不完全なデータの導入
B. ラベル付けに疑問のあるデータ
C. AIモデルのトレーニングにおける透明性の欠如がユーザーの不信感を引き起こしている
D. データプライバシー規制違反による法的罰則
正解: **(**正解を表示します**)**
同意なしにソーシャルメディアデータを使用することは、深刻な法的および倫理的問題を引き起こします。AAIA™マニュアルによると、最大の危険は「データプライバシー規制（GDPRやCCPAなど）の違反」であり、重大な法的罰則、モデルの強制削除、訴訟につながる可能性があります。データが「公開」されている場合でも、プライバシー法は、明確な法的根拠（同意など）なしに、自動意思決定やプロファイリングのために個人情報を使用することを制限することがよくあります。データ品質（オプションA）とラベル付け（オプションB）は運用上のリスクですが、規制違反とその結果生じる事業許可の喪失ほど、組織にとって存続の危機となるものではありません。

質問: **132**
監査の観点から見て、次のうちどれがAIガバナンスプログラムの目的を最もよくサポートしますか？
A. AI倫理に関するすべての関係者の役割、責任、およびトレーニングを明確にする
B. AI倫理委員会または責任あるAI審査委員会の設置
C. 潜在的なアルゴリズムバイアスを記録するためのAIリスク登録簿の開発
D. モデルの解釈可能性、透明性、回復力に関するAIポリシーの定義
正解: **(**正解を表示します**)**
役割（オプションA）、委員会（オプションB）、登録簿（オプションC）は組織の重要な構成要素ではあるが、「AIポリシー」そのものがガバナンスの目的を最も包括的にサポートするものである。
ポリシーは、AIの構築と管理方法に関する「強制力のある基準」を提供するものです。具体的には、解釈可能性、透明性、回復力に関するポリシーは、組織のAIシステムが監査可能で、公平かつ安定していることを保証します。ISACAによると、ガバナンスプログラムは、AI開発に必要な安全策を提供するために、これらの技術的および倫理的な柱に基づいている必要があります。ポリシーは、委員会や利害関係者が意思決定プロセスを行う際の指針となる「真実の源泉」として機能します。

質問: **133**

導入前のリスク評価において、AIモデルが組織の許容リスクを超える重大なバイアスリスクと潜在的な危害をもたらすと判断されました。次のうち、最も適切な対応はどれですか？
A. リスクを安全に管理できるようになるまで、配備を延期する。
B. モデルの学習に使用するデータを強化する。
C. 例外について取締役会の承認を得る。
D. リスク許容度を再検討し、それが適切であることを確認する。
正解: **(**正解を表示します**)**
AAIA™学習ガイドでは、AIモデルが組織の事前定義されたリスク許容度を超えるリスクをもたらす場合（特に倫理的な危害や偏見が生じる場合）、適切な安全対策が講じられるまで導入を延期すべきであると提言しています。このアプローチにより、法的責任を回避し、ステークホルダーの信頼を維持することができます。
「AIのリスクが許容範囲を超えた場合、組織は是正措置によってリスクが許容レベル内に収まるまで、導入を一時停止しなければならない。リスク軽減策を講じずに導入を進めることは、健全なガバナンス原則に反する。」データの改善（B）は役立つかもしれないが、差し迫ったガバナンス上の懸念には対処できない。リスク許容度（D）は、欠陥のあるシステムに合わせて調整すべきではない。したがって、Aが正しい選択肢である。
参考資料：ISACA Advanced in AI Audit™ (AAIA™) 学習ガイド、セクション：「AIガバナンスとリスク管理」、サブセクション：「リスク評価と実装意思決定」

質問: **134**
ドリフト閾値や公平性指標閾値など、AI固有の主要リスク指標（KRI）を設定する主な目的は何ですか？
A. マーケティング要件を満たすため
B. 被害が発生する前に調査や是正措置を促す、早期かつ測定可能な警告信号を提供する。
C. クラウドコンピューティングのコストを削減するため
D. 人間の監視の必要性を排除するため
正解: **(**正解を表示します**)**
KRI（重要リスク指標）は、抽象的なリスク（ドリフトやバイアスなど）を測定可能な閾値に変換し、それに基づいて積極的な対策を講じることで、問題がインシデントに発展する前にリスク管理を可能にします。

質問: **135**
AIモデル用のデータフレームにデータを初期的に入力する際に、以下のうちどれが最も重要ですか？
A. 相関関係や外れ値を特定する箱ひげ図、ヒストグラム、散布図、ベン図
B. データをトレーニングデータセットとテストデータセットに分割するためのコード
C. 探索的データの分析で、誤ったデータ型、ヌル値、重複エントリをチェックします。

D. モデルへのデータ属性の組み込み、除外、または後からの削除に関する承認済みのリスク評価
正解: **C** (コメントを発表する)
探索的データ分析（EDA）は、AIモデル開発の初期段階において非常に重要です。
AAIATM学習ガイドによると、欠損値、誤ったデータ型、重複データの特定などを含むEDA（探索的データ分析）を実行することで、モデルに入力されるデータがクリーンで信頼できるものとなることが保証される。
初期データフレームは、データ品質の問題を明らかにするために、徹底的な探索的データ分析（EDA）の対象となるべきです。これらの問題は、早期に対処しないと、モデルのトレーニングと予測精度に深刻な影響を与える可能性があります。」

質問: **136**
ある企業が、トレーニングデータやアーキテクチャに関する情報が不明なまま、サードパーティのAIベンダーのモデルを導入した場合、監査において最も懸念される点は何でしょうか？
A. ベンダーロックイン
B. ライセンス費用の増加
C. 透明性の欠如により、偏り、逸脱、または説明可能性を評価できない。
D. 推論速度が遅い
正解: **C** (コメントを発表する)

有効的な**AAIA**問題集はJPNTest.com提供され、**AAIA**試験に合格することに役に立ちます！JPNTest.comは今最新**AAIA**試験問題集を提供します。JPNTest.com AAIA試験問題集はもう更新されました。ここで**AAIA**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/AAIA-mondaishu　**328**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **137**
AIモデルの出力におけるバイアスを効果的に制御するための最良の方法は、次のうちどれですか？
A. モデル開発プロセスの技術的な詳細は透明性があります。
B. 組織のAIポリシーには、公平性に関する明確な定義が含まれています。
C. モデルのトレーニングは、現実世界の人間の意思決定を含むデータに限定されます。
D. さまざまな人口統計グループにおける精度範囲は類似している。
正解: **D** (コメントを発表する)

質問: **138**

IS監査担当者は、AIモデルがテストデータよりも訓練データにおいて著しく優れた結果を達成したと指摘している。
開発後、品質保証（QA）チームが、すべての入力変数とパラメータが技術設計と一致していることを確認します。この活動を最も適切に説明しているのは次のうちどれですか？
A. モデル検証
B. モデル検証
C. モデルテスト
D. モデルチューニング
正解: **(**正解を表示します**)**
ISACA AAIA™フレームワークでは、「検証」と「妥当性確認」を区別しています。「検証」は、システムが「正しく構築された」かどうか、つまりコード、パラメータ、アーキテクチャが設計ドキュメントと一致しているかどうかを確認する品質保証プロセスです。「妥当性確認」（オプションA）は、「正しいシステム」が構築されたかどうか、つまりモデルが未知のデータに対して実際に正しく動作し、ビジネス目標を満たしているかどうかを確認します。テスト（オプションC）はパフォーマンスギャップを特定しますが、モデルの構成を技術設計図と照らし合わせて監査するという具体的な行為は、検証活動です。

質問: **139**
IS監査担当者がAIモデルの変更管理文書をレビューしています。次のうち、モデルにとって最も大きなリスクとなるのはどれでしょうか？
A. 同じシード値を使用するモデルを比較するA/Bテスト
B. モデルはトレーニングセットで調整されました
C. 異なるシード値を用いたモデルを比較するA/Bテスト
D. モデルは同じデータ分割で学習されました
正解: **(**正解を表示します**)**
AI開発において、「シード」は、重み初期化などのランダムなプロセスが再現可能であることを保証します。A/Bテストで異なるシードを使用して2つのモデルを比較した場合、監査者はパフォーマンスの違いがモデルの変更によるものなのか、単に重みの初期化方法における「偶然の幸運」によるものなのかを判断できません。これはテスト結果を無効にします。「公平な」同条件での比較を行うには、シードは一貫している必要があります。トレーニングセットでのチューニング（オプションB）は標準的ですが、過学習のリスクがあります。しかし、テストにおける科学的制御の欠如（オプションC）は、変更管理プロセスの整合性に対するより直接的なリスクとなります。

質問: **140**
ある組織が調達チームと在庫管理チームにAIを導入しようとしており、関係者からはAIによって職を失うのではないかという懸念が上がっている。情報システム監査担当者が潜在的な悪影響が最小限に抑えられたかどうかを評価するための最良の方法は次のうちどれか？

A. 人間中心設計の実践をレビューし、それらがどのように考慮されたかを判断する。
B. 短期および長期のマイルストーンについて、AIロードマップを確認する。
C. プロジェクト管理チームがエンゲージメント活動でどのようにフィードバックを収集したかをレビューします。
D. AIが組織にどのような影響を与える可能性があるかについての現状評価をレビューする。
正解: **A (**コメントを発表する**)**
人間中心設計（HCD）は、ステークホルダーのニーズ、倫理的側面、社会的影響をAIシステム開発に統合することに重点を置いています。AAIA™学習ガイドでは、HCDが従業員への悪影響を最小限に抑え、包括的な設計を確保する上で果たす役割を強調しています。
監査担当者は、AIシステムの設計プロセスに人間中心のアプローチが取り入れられているかどうかを検証すべきである。特に、雇用や重要な人的役割に影響を与えるアプリケーションについては、人間中心設計（HCD）が責任ある導入を保証する。」フィードバック収集（C）と影響評価（D）は有用な背景情報を提供するが、Aは設計レベルでの倫理的影響の軽減に直接的に取り組んでいる。
参考資料：ISACA Advanced in AI Audit™ (AAIA™) 学習ガイド、セクション：「AIにおける倫理的および法的考慮事項」、サブセクション：「人間中心のAIと労働力への影響」

質問: **141**
自動車メーカーは、AIモデルを使用して車両のメンテナンスニーズを予測しています。IS監査担当者は、利害関係者に対してAIモデルの決定を最も効果的に検証するために、次のうちどの手法を適用できますか？
A. ニューラルネットワークの可視化を用いて、AIモデルが層を通してどのようにデータを処理するかを示す。
B. K平均法アルゴリズムを用いて、走行距離またはエンジン温度に基づいて車両をグループ化し、メンテナンスパターンを分析する
C. サポートベクターマシン（SVM）を用いて、メンテナンスの緊急度に基づいて車両を分類する
D. 局所的に解釈可能なモデル非依存型説明（LIME）を用いて、特定の機能が予測にどのように寄与するかを分析する
正解: **(**正解を表示します**)**
LIME（Local Interpretable Model-Agnostic Explanations：局所的に解釈可能なモデル非依存型説明）は、複雑なモデルの挙動を局所領域における単純で解釈可能なモデルで近似することにより、個々のAI予測を説明するための主要なツールです。AAIATM学習ガイドでは、LIMEが非技術系の関係者に対して透明性と解釈可能性を提供する上で非常に効果的であると強調しています。
「LIMEは、監査担当者が特定の入力機能がAIの意思決定にどのように影響を与えたかを実証することを可能にし、特に規制対象または影響の大きい状況において、信頼と利害関係者の理解を促進します。」

質問: **142**
ある組織が、求職者の選考にAI採用プラットフォームを導入しました。情報システム監査担当者は、このプラットフォームの判断がモデルのバイアスによって影響を受ける可能性があることを指摘しました。監査担当者が推奨するリスク軽減策として最適なのは、次のうちどれでしょうか？
A. 採用が確定する前に、AIが生成したすべての採用決定について手動によるレビューを義務付ける。
B. トレーニングデータが公平性とコンプライアンスを検証できるまで、AIシステムの使用を一時停止する。
C. 包括性と公平性が認証された外部データセットを使用して、AIモデルを再学習します。
D. AIシステムのバイアスを定期的にテストし、必要に応じてパラメータを調整するプロセスを実装する。
正解: **D** (コメントを発表する)

質問: **143**
AIにおいてニューラルネットワークを利用する主な目的は以下のとおりです。
A. ユーザーインターフェースを改善する。
B. 計算能力を向上させる。
C. 人間の意思決定を模倣する。
D. メンテナンスコストを最小限に抑える。
正解: **C** (コメントを発表する)
ニューラルネットワークは、人間の脳が情報を処理する方法を模倣するように設計されており、AIシステムが複雑なパターンを識別し、データ入力に基づいて意思決定を行うことを可能にします。AAIATM学習ガイドでは、ニューラルネットワークは認知機能を模倣する深層学習アーキテクチャの中核をなすものとして定義されています。
ニューラルネットワークは、人間の脳の相互接続性と学習プロセスをシミュレートします。この機能により、AIシステムは非構造化データを処理し、画像認識、自然言語処理、予測分析などのタスクを実行できるようになります。

質問: **144**
IS監査担当者が組織のデータガバナンスフレームワークを監査しています。主な目的は、信頼できるAIシステムをサポートするためにデータ管理の実践が標準化されていることを保証することです。監査担当者が最も重視すべき事項は次のうちどれでしょうか？
A. 保存データの保持
B. データの移植性
C. モデル学習のためのデータ活用法
D. データ管理における説明責任
正解: **D** (コメントを発表する)

データ管理における説明責任（オプションD）は、最も重要な考慮事項です。AAIA™学習ガイドでは、「データ管理活動における明確な役割、責任、および所有権は、コンプライアンス、トレーサビリティ、およびポリシーとコントロールの一貫した適用を保証するため、信頼できるAIシステムにとって不可欠である」と強調しています。データの保持、移植性、およびトレーニングの実践は重要ですが、説明責任は、他のすべてのガバナンス実践の実施と監視の基礎となります。
参考資料：ISACA Advanced in AI Audit™ (AAIA™) 学習ガイド、セクション：「AIにおけるデータガバナンスの説明責任」

質問: **145**
以下のテスト手法のうち、組織のデータガバナンスプログラムがAIモデルのトレーニングと展開におけるデータ品質と整合性を効果的に保証しているかどうかを最も適切に検証できるのはどれですか？
A. AIモデルの失敗による影響を評価するための事業影響分析（BIA）を実施する
B. 組織のAIソフトウェア開発ライフサイクル文書のレビュー
C. データソースのトレーサビリティを検証するためのデータ系統の評価
D. モデルの脆弱性を特定するための侵入テストを実施する
正解: **C** (コメントを発表する)

質問: **146**
IS監査担当者は、多様な階級の代表性を確保するための少数派データの不足が原因で、データ品質に問題があることを特定しました。この問題を解決するための最適な推奨事項は次のうちどれですか？
A. データを合成することでデータを拡張する。
B. モデル選択を変更します。
3. リスク受容について文書化する。
C. 利用可能なデータを再ラベル付けします。
正解: **A** (コメントを発表する)
データセットに「少数派クラス」（例えば、希少疾患や特定の人口統計グループ）の十分な例がない場合、モデルは多数派クラスに偏った傾向を示す可能性が高くなります。最適な技術的推奨事項は、「合成によるデータ拡張」（SMOTEやGANなどの手法を使用）です。合成データ生成は、人工的ではあるものの統計的に現実的な少数派サンプルを作成し、入手が困難な場合もある実世界のデータを必要とせずに、モデルがこれらのグループの特徴を学習できるようにします。

質問: **147**
保険会社が保険料率を設定するためにAIモデルを使用しています。公平性に関するAI関連のポリシーに沿うために、最初にとるべき行動は次のうちどれですか？
A. 代替AIモデルをトレーニングし、バイアスを主要モデルと比較する

B. AIモデルのトレーニングデータをレビューして、潜在的なバイアスを特定する
C. 潜在的なバイアスに対処するため、AIモデルのトレーニングデータセットを修正する
D. AIモデルが提示したプレミアム料金について、顧客が異議を申し立てられるようにする
正解: **(**正解を表示します**)**
AAIAのガイダンスでは、公平性の評価はトレーニングデータから始めるべきだと述べている。なぜなら、バイアスはデータの選択、サンプリングの不均衡、ラベル付けの不整合、またはソースデータに埋め込まれた過去の差別によって最も一般的に生じるからである。
したがって、最初の行動方針は、トレーニングデータ（オプションB）をレビューして以下を特定することです。
* 人口分布の偏り
* 欠落している、または過小評価されている集団
* 機密属性の不適切な使用
* ラベルが間違っているか、変数が正しくエンコードされていない
差別を助長する可能性のある過去の決定
組織は、バイアスの存在とその性質を特定した後で初めて、再トレーニング（C）や代替モデルの動作の比較（A）などの是正措置に進むことができます。
顧客が保険料に異議を申し立てることを認めること（D）は、決定後の救済措置であり、公平性を評価するステップではない。
AAIAは、モデルや出力を調整する前に、バイアスの根本原因であるトレーニングデータに対処することを重視している。
参考文献：
AAIAドメイン5：公平性、バイアスの特定、倫理的なAI原則
AAIAドメイン2：データガバナンスとインプット評価

質問: **148**
AIモデルがビジネス目標を達成しているかどうかを評価する際に、以下の主要業績評価指標（KPI）のうち、最も重要なものはどれですか？
A. AIモデルトレーニングに必要なリソースのコスト
B. AIモデルとインタラクションしているユーザー数
C. AIモデルの再学習頻度
D. 実際の結果を予測する際のAIモデルの精度
正解: **(**正解を表示します**)**
あらゆるAIシステムの主な目的は、ビジネス上の意思決定を支援する予測や分類を提供することである。
AAIA™学習ガイドでは、モデルの精度、特に実際の成果と照らし合わせて検証した場合の精度が、AIが組織目標を効果的にサポートしているかどうかを判断する最も信頼できる指標であると強調しています。
精度、適合率、再現率は、モデルが意図した目標に沿って動作しているかどうかを示す基本的な指標です。出力が正しければ、高いユーザーエンゲージメントや再学習頻度は効果的

な意思決定支援を保証するものではありません。」コストとユーザー数は有用な運用上の洞察を提供しますが、AIのパフォーマンスが戦略目標と整合しているかどうかは反映しません。したがって、この文脈ではDが最も重要なKPIとなります。
参考資料：ISACA Advanced in AI Audit™ (AAIA™) 学習ガイド、セクション：「AIの運用とパフォーマンス」、サブセクション：「AIの指標とビジネスとの整合性」

質問: **149**
AIチームが顧客を支援するための自然言語処理（NLP）チャットボットを開発しています。収集されたデータには、非公式な会話や複数の言語が含まれています。どの前処理ステップが最も重要ですか？
A. 辞書を使って非公式な言葉遣いを標準化し、翻訳を取り入れる。
B. エンティティ認識を実行して重要な情報を抽出します。
C. トークン化とステミングを適用して複雑さを軽減します。
D. 複雑さを避けるため、英語以外のデータをすべて削除します。
正解: **(**正解を表示します**)**
自然言語処理（NLP）において、学習の質は入力データの「標準化」に大きく左右されます。非公式な表現（スラング、誤字脱字など）や複数の言語が混在すると、ノイズが多くなり、モデルが意味を学習しにくくなります。辞書を使ってテキストを正規化し、翻訳サービスを利用して一貫性のあるデータセットを作成することが、最も基本的なステップです。

質問: **150**
IS監査担当者が、生成型AIツールを使用して4,000行のバッチで傾向を特定する財務システムを監査しています。ただし、生成型AIツールには3,000トークンの制限があります。以下のうち、最も懸念されるのはどれですか？
A. AIは価値の高いエントリを優先します。
B. AI の出力は最初の 3,000 トークンに偏ります。
C. AIはデータセットを拒否し、データを分析しません。
D. AIはデータセットの一部のみを処理します。
正解: **(**正解を表示します**)**

質問: **151**
畳み込みニューラルネットワーク（CNN）モデルをトレーニングするために利用できる詳細な画像データセットが限られている場合、以下のどの手法を使用するのが最適でしょうか？
A. データセットをトレーニングセットとテストセットに50/50で分割する
B. 少数派クラスのサンプリング不足
C. オープンソースモデルからの転移学習
D. 現在のデータセットの複製
正解: **(**正解を表示します**)**

データが不足している場合、ディープCNNをゼロからトレーニングすると過学習が発生する可能性が高くなります。 転移学習」を使用すると、組織は大規模データセット（ImageNetなど）で以前にトレーニングされたモデルを取得し、 微調整」することができます。
 特定の小規模データセット向けです。モデルは既に基本的な形状やテクスチャを認識する方法を知っているため、特定の新しいカテゴリを学習するために必要なデータははるかに少なくて済みます。これは、医療画像処理や特殊な製造監査において一般的で非常に効果的な手法です。データの複製（オプションD）は新しい情報を追加せず、過学習につながるだけです。」

有効的な**AAIA**問題集はJPNTest.com提供され、**AAIA**試験に合格することに役に立ちます！JPNTest.comは今最新**AAIA**試験問題集を提供します。JPNTest.com AAIA試験問題集はもう更新されました。ここで**AAIA**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/AAIA-mondaishu 328問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **152**
IS監査担当者は、トレーニング、検証、テストデータセットで使用されたレコードの合計数が、元のデータセットのレコード総数を超えていることに気づきました。監査担当者にとって最も重要な判断事項は次のうちどれですか？
A. トレーニング、検証、テストデータセットが正しい順序で作成されたかどうか
B. データセット内の重複レコードの利用によりデータ漏洩が発生したかどうか
C. トレーニングデータセットで十分な数のレコードが使用されたかどうか
D. 検証データセットがトレーニングデータセットと同じ数のレコードを使用しているかどうか
正解: **B** (コメントを発表する)
トレーニングセット、検証セット、テストセットの合計サイズが元のデータサイズを超える場合、レコードが複数のセットで再利用されている可能性が示唆されます。これはデータリークにつながり、トレーニング中にモデルがテスト情報や検証情報にアクセスできてしまうため、パフォーマンス指標が過度に楽観的になる可能性があります。
データ漏洩は、意図しないデータ重複を引き起こすため、モデル評価を無効にする。
監査担当者は、トレーニングセット、検証セット、テストセットが厳密に区分されていることを確認しなければならない。

質問: **153**
組織のAIベンダー管理を監査する際に、以下の評価基準のうち、最も優先順位が高いのはどれですか？
A. 説明可能なAIの意思決定と監査証跡のためのモデル解釈可能性
B. AIベンダーのパフォーマンスを測定するために使用されるサービスレベル目標（SLO）

C. 自然言語処理（NLP）によって生成されたサプライヤー契約
D. 効率的なAIモデル干渉のためのハードウェア要件
正解: **(**正解を表示します**)**
AIをアウトソーシングする場合、組織はモデルの決定に対する責任を保持します。監査担当者にとって最優先事項は、「解釈可能性」、つまりベンダーがモデルの根拠を説明するツールやドキュメントを提供できる能力を確保することです。これがなければ、組織は透明性に関する規制要件（GDPRの説明を受ける権利など）を満たすことも、ベンダーのモデルに偏りがないことを検証することもできません。SLO（オプションB）は運用稼働時間にとって重要ですが、関連する倫理的または法的リスクを軽減するものではありません。
第三者によって提供される「ブラックボックス」アルゴリズム。

質問: **154**
組織のAI統合が、その組織の全体的なテクノロジー戦略と整合していることを示す最良の証拠は、次のうちどれですか？
A. IT部門には、AIの専門知識を持つ多くの個人貢献者がいます。
B. 経営陣はイノベーションの文化を推進する。
C. 組織はAI利用に関する方針を策定し、周知徹底させている。
D. AIシステム向けに主要業績評価指標（KPI）が定義されています。
正解: **D** (コメントを発表する**)**
AI統合とテクノロジー戦略の整合性を示す最良の証拠は、AIシステムに対して明確なKPI(A)が定義され、戦略目標、測定可能な成果、ガバナンスの監視と結び付けられていることである。
KPIは、AIイニシアチブが監視され、パフォーマンスが評価され、成果が企業価値と一致していることを示す。
ポリシー（B）は基礎となるものですが、戦略的な整合性を示すものではありません。イノベーション文化（C）は広範かつ主観的なものです。AIの専門知識（D）は能力を示すものであり、整合性を示すものではありません。AAIAは、指標、モニタリング、ガバナンスダッシュボードを通じて、AIの成果をビジネス目標に結びつけることを重視しています。
参考文献：
ISACA、AAIA試験内容概要 - ドメイン1：AIガバナンスと戦略の整合性。

質問: **155**
攻撃者がAIモデルから機密情報を抜き取った場合、最初に行うべきことは次のうちどれですか？
A. レート制限とクエリ制限を実装して、悪用試行を減らします。
B. 攻撃経路が特定されるまで、影響を受けたシステムを隔離する。
C. より安全なアーキテクチャを使用してAIモデルを再構築する。
D. 規制当局および影響を受ける利害関係者に、データ侵害の可能性を通知する。
正解: **(**正解を表示します**)**

AIATMの学習ガイドによると、データ漏洩攻撃が確認または疑われる場合、最初にとるべき行動は封じ込めである。影響を受けたシステムを隔離することで、さらなる悪用を防ぎつつ、漏洩源の安全な調査が可能となる。
「AI関連のデータ侵害が発生した場合、最初の対応では脅威の封じ込めを最優先事項としなければならない。」
影響を受けたシステムを直ちに隔離することで、さらなる被害を軽減し、管理されたフォレンジック分析を支援することができます。

質問: **156**
モデル開発チームとは独立した「モデル検証」機能の目的を最も適切に説明しているのは、次のうちどれですか？
A. モデルの展開を加速するため
B. 展開前後のモデル性能、前提条件、および限界について、客観的かつ偏りのない評価を提供する。
C. 開発コストを削減するため
D. モデルのソースコードを作成する
正解: **(**正解を表示します**)**
独立したモデル検証は、リスク管理における「第二防衛線」の概念を反映している。つまり、モデルを構築する者と、それを検証し承認する者を分離することで、利益相反や確証バイアスを軽減できる。

質問: **157**
AIベースのアプリケーションシステムに影響を与える最悪のサービス中断シナリオを最も効果的に軽減できる制御策は次のうちどれですか？
A. 主要リスク指標（KRI）を定期的に更新する
B. 混乱発生時のキルチェーンプロセスの実施
C. 災害復旧計画（DRP）に、AIによる障害に関する様々なシナリオを含める
D. 定期的な卓上運動の実施
正解: **(**正解を表示します**)**

質問: **158**
IS監査担当者が、トレーニングセット、検証セット、テストセットのレコード数を合計すると、元のデータセットのレコード総数を超えていることに気づきました。最大のリスクは何ですか？
A. データセットが間違った順序で作成されました。
B. 重複したレコードからデータ漏洩が発生しました。
C. トレーニングに十分な数のレコードが使用されませんでした。
D. 検証データセットはトレーニングセットよりも大きい。
正解: **(**正解を表示します**)**

適切なAIパイプラインでは、元のデータは互いに素な集合に「厳密に分割」されなければなりません。部分集合の合計が元のデータ数を超える場合、一部のレコードが複数の集合間で「再利用」されたことを意味します。
これは「データ漏洩」につながり、モデルがトレーニング段階でテストデータや検証データを「見てしまう」ことになります。その結果、モデルのパフォーマンス指標が人為的に過大評価され、誤った精度感を与えてしまいます。ISACA AITM学習ガイドでは、データ漏洩を「モデル評価失敗」の主な原因として挙げており、すべてのテスト結果が無効になる原因となっています。

質問: **159**
生成型AIモデルの説明可能性にとって、最も大きな障壁となるのは次のうちどれですか？
A. モデル学習に使用されるデータセット内のバイアス
B. アルゴリズム機能の急速な進化
C. 利害関係者グループ間の連携不足
D. 生成AIツールに関するスタッフの経験不足
正解: **B** (コメントを発表する)
現代の生成型AIアーキテクチャの急速な進化（オプションB）は、説明可能性にとって最大の障壁となっている。
LLM、拡散モデル、トランスフォーマーベースのアーキテクチャといった複雑な深層学習モデルは、数百万、数十億ものパラメータを含むため、出力がどのように生成されるかを正確に判断することは非常に困難です。
AAIAは、説明可能性に関する課題が生じる理由として、以下の点を挙げている。
* モデル構造は非常に複雑です
* パラメータ間の相互作用は非線形である
* 内部表現は人間が解釈できるものではない
* 継続的な更新により、ドキュメントが古くなってしまうことがあります。
* トレーニングデータと潜在表現は不透明な推論チェーンを作成します。バイアス（A）は公平性に影響を与えますが、説明可能性には影響しません。
利害関係者の合意（C）はガバナンスの問題である。
スタッフの経験不足（D）は、構造的な障壁ではなく、研修の問題である。
技術的な複雑さとモデル進化のスピードが主な障害となっている。
参考文献：
AAIAドメイン5：説明可能性の課題
AAIAドメイン1：高度なAIモデルアーキテクチャ

質問: **160**
従来の監査方法と比較して、AI監査技術を使用する最大の利点は、AI監査技術が以下のことを可能にする点です。
A. 人間の介入の必要性を排除する。

B. 規制を完全に遵守すること。
C. 複雑なデータパターンを識別する。
D. データバイアスを大幅に低減します。
正解: **C** (コメントを発表する)
AI監査技術は、複雑なデータパターン（オプションC）の特定に優れており、これが手動または従来の監査手法に対する主な利点です。AAIATM学習ガイドには、「AIベースの監査ツールは、膨大な量のデータを高速かつ詳細に処理し、人間の監査員には見えない、あるいは手動では発見できない可能性のある異常、傾向、または関係性を検出できます」と記載されています。AIは人間の関与を完全に排除するものではなく、コンプライアンスやバイアスの排除を保証するものでもありませんが、大規模で多次元的なデータセット内の複雑なパターンを分析することができます。

質問: **161**
IS監査担当者が、生成型AIが同じデータセットから異なる投資推奨を返す可能性があることを認識しておくべき主な理由は、次のうちどれですか？
A. サーバーは定期的に再構成されます。
B. 計算論理は確率に基づいています。
C. ニューラルノードへのアクセスは、プロセスが実行されるたびに変化します。
D. リスクプロファイルの定量化には限界が生じる可能性があります。
正解: (正解を表示します)

質問: **162**
IS監査担当者が、生成型AIツールを使用して4,000行のバッチで傾向を特定する財務システムを監査しています。ただし、生成型AIツールには3,000トークンの制限があります。以下のうち、最も懸念されるのはどれですか？
A. AIはデータセットの一部のみを処理します。
B. AIは価値の高いエントリを優先します。
C. AIはデータセットを拒否し、データを分析しません。
D. AIの出力は最初の3,000トークンに偏ります。
正解: **D** (コメントを発表する)
大規模言語モデルなどの生成型AIツールには、トークン数の制限があり、1回のプロンプトで処理できる入力量が制限されることがよくあります。AAIA™学習ガイドによると、入力がトークン数の制限を超えると、モデルは最初の部分のみを処理するため、初期の入力に基づいて偏った出力が生成されます。
「生成型AIシステムにおけるトークン制限は、入力処理が不完全になる可能性があり、モデルの出力がデータの先頭に偏り、解釈上のバイアスが生じる可能性があります。監査担当者は、出力がデータセット全体を反映しているかどうかを評価する必要があります。」オプションAとCは副作用について説明していますが、Dは入力の切り捨てによる最も重大なリスクと出力の歪みを特定しています。

参考資料：ISACA Advanced in AI Audit™ (AAIA™) 学習ガイド、セクション：AIの運用とパフォーマンス」、サブセクション：生成型AIモデルの限界」

質問: **163**
AIシステムの変更管理手順を調査しているIS監査担当者が、モデルの再トレーニング前にトレーニングデータの検証および確認プロトコルに一貫性がないことに気づきました。この状況において、最も重大なリスクは次のうちどれでしょうか？
A. データ入力の不整合によるAIモデルの複雑化
B. モデルトレーニング文書の不備による不遵守
C. データの破損または品質低下によるシステム信頼性の低下
D. 手続き上の非効率性によるAIモデルの再学習の遅延
正解: **(**正解を表示します**)**
トレーニングデータの検証が不完全な場合、最も深刻なリスクは、AIモデルが不正確、不完全、偏りのある、または破損したデータから学習してしまう可能性があることです。これは直接的にシステムの信頼性の低下（オプションC）につながり、不正確な予測、高いエラー率、偏り、または不安定な動作として現れます。
AAIAは、モデルの動作はトレーニングデータの整合性に完全に依存しているため、再トレーニング前のデータ検証が最も重要な管理策の一つであることを強調しています。データの品質と正確性が保証できない場合、結果として得られるモデルの出力は信頼性を失い、コンプライアンス、運用上の意思決定、およびユーザーの信頼を損なう可能性があります。

質問: **164**
ブラウザ拡張機能としてAIシステムを実装する際に、過剰な主体性を軽減するための最適な推奨事項は次のうちどれですか？
A. ブラウザ拡張機能の機能を最小限に抑えます。
B. ブラウザ拡張機能へのユーザーアクセスを削除します。
C. ブラウザ拡張機能の機能を最大限に活用する。
D. オープンソースのブラウザ拡張機能を使用する。
正解: **A (**コメントを発表する**)**
過剰な自律性とは、AIシステムが人間の適切な監視なしに意思決定を行うなど、過度に自律的に動作する場合に発生します。ブラウザ拡張機能においてこれを軽減するための最善のアプローチは、機能を最小限に抑えること（A）であり、拡張機能が厳密に定義された制御された動作のみを実行するようにします。これは、AIの自律性を制限し、最小権限の原則を適用し、不要な動作を制限するというAAIAのガイダンスに合致しています。
ユーザーアクセスを完全に排除する（B）は過度に制限的である。機能を最大限に高める（C）はリスクを高める。オープンソースの拡張機能（D）は透明性を向上させるが、過剰な権限行使を本質的に抑制するものではない。範囲を制限することが、最も的を絞った効果的な緩和策である。

参考文献：
ISACA、AAIA試験内容概要 - ドメイン1 :ガバナンス、AI自律性、およびリスク管理。

質問: **165**
AIシステムのリスク評価において、データドリフトが主要なリスクとして特定されました。以下のうち、最適な対応策はどれですか？
A. リスクを文書化し、継続的な監視を実施する。
B. 同じデータセットを使用して、モデルをすぐに再学習します。
C. トレーニングデータをアーカイブし、デプロイに進みます。
D. リスクがなくなるまでAIシステムを無効化する。
正解: **(**正解を表示します**)**
データドリフトとは、入力データの統計的特性が時間とともに変化し、AIモデルがますます不正確または偏った結果を生成するようになる現象である。
正しい対応策は、リスクを文書化し、継続的なモニタリングを実施することである (A)。理由は以下のとおりである。
ドリフトは一度の修正ではなく、継続的な検出が必要です。
* 再学習を早すぎると、問題が悪化する可能性がある（特に同じデータセットを使用する場合）。
* システムを無効にする (D) ことは、ドリフトによって安全でない決定が下されない限り、過度に混乱を招く。
* 監視なしで展開を続けると (C) パフォーマンスが低下するリスクが高まります。AAIA は、ドリフト監視ダッシュボード、アラートメカニズム、再トレーニングトリガーを AI 運用の必須制御として強調しています。
参考文献：
AAIAドメイン2 :AI運用 - モニタリング、ドリフト検出、ライフサイクルメンテナンス

質問: **166**
教師ありAI学習モデルは、アルゴリズムのトレーニングに主に次のうちどれを使用しますか？
A. ラベルなしデータセット
B. クラスタ化されたデータセット
C. ラベル付きデータセット
D. ランダム化データセット
正解: **(**正解を表示します**)**
教師あり学習は、ラベル付きデータセットを用いてモデルを訓練する、機械学習の基礎的な手法です。AAIATM学習ガイドによると、ラベル付きデータには入力特徴量と正しい出力値が含まれており、モデルがマッピング関数を正確に学習することを可能にします。
教師あり学習では、モデルは訓練データで提供される入出力ペアから学習します。この方法により、分類や回帰などの予測モデリングタスクが可能になります。」ラベルなしデータ

A)は教師なし学習で使用され、クラスタリングデータ B)はデータタイプではなく手法であり、ランダム化データ D)はラベル付けではなく分布戦略を指します。したがって、ラベル付きデータが正解です。

有効的な**AAIA**問題集はJPNTest.com提供され、**AAIA**試験に合格することに役に立ちます！JPNTest.comは今最新**AAIA**試験問題集を提供します。JPNTest.com AAIA試験問題集はもう更新されました。ここで**AAIA**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/AAIA-mondaishu 328問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **167**
研究機関が科学データの分析に生成型AIモデルを使用しているかどうかを監査する際、幻覚的な結果を防止し、出力の正確性を確保するために、以下のうちどれを評価することが最も重要ですか？
A. 入力データの完全性と正確性を検証するデータ監査の頻度
B. データ品質の維持に役立つデータ匿名化プロセスの有効性
C. 生成AIモデルのためのアルゴリズムは、処理前にデータバイアスを検出して修正するように設計されています。
D. 生成AIモデルへの入力データの適切性と関連性を確保するための措置
正解: **(**正解を表示します**)**

質問: **168**
IS監査担当者が、組織のAIシステムの精度が要求される閾値を下回っていることを発見し、より正確な結果を得るために複数のモデルを相互参照するよう経営陣に勧告しました。これは、どのようなタイプのリスク対応の例でしょうか？
A. 回避
B. 受容
C. 転送
D. 緩和
正解: **(**正解を表示します**)**
リスク軽減とは、リスクの発生確率や影響を許容できるレベルまで低減するための管理策や対策を実施することです。このシナリオでは、モデルが精度の閾値を満たせないことが、パフォーマンスと運用上のリスクとなります。監査人は、モデルアンサンブルの使用や相互参照（複数のモデルが同じ入力を評価する）を推奨することで、システムの出力の信頼性を向上させるための技術的管理策を提案しています。これにより、システムを完全に排除することなく（回避）あるいはリスクを第三者に移転することなく（移転）誤った判断のリスクを低減できます。リスク軽減は、既存のユースケースを維持しながらAIのパフォーマンスを向上させるための標準的な対応策です。

質問: **169**
医療機関がデータクラスタリングを用いて、患者の病歴に基づいてグループ分けを行い、個別の治療推奨を行っています。この手法に伴う最大のプライバシーリスクは次のうちどれでしょうか？
A. クラスタリングにはより多くのデータが必要となり、プライバシー侵害のリスクが高まります。
B. データ内の無関係な特徴は、不正確または偏った治療につながる可能性があります。
C. クラスタリングはモデルの複雑さを増大させ、データの匿名化を困難にします。
D. クラスターは、情報の提示方法によっては、機密性の高い個人情報を明らかにする可能性があります。
正解: **(**正解を表示します**)**

質問: **170**
監査を支援するために、承認済みの生成型AIツールにソースデータを入力すべきかどうかを判断する際に、IS監査担当者が取るべき最も重要な行動は次のうちどれですか？
A. 情報が信頼できるかどうかを判断する。
B. AIモデルの幻覚が発生したかどうかを判定します。
C. ツールが最新モデルを活用していることを確認してください。
D. ツールがプライバシーに関する通知を提供していることを確認します。
正解: **(**正解を表示します**)**

質問: **171**
ある小売業者のAI価格設定エンジンが、特定の地域で異常に大きな割引を推奨している。監査の結果、モデルのトレーニングに使用された過去の販売データのほとんどが大都市圏からのものであり、小規模地域は販売記録がほとんど、あるいは全くなかったことが判明した。この問題の最も可能性の高い原因は次のうちどれか？
A. 地域識別子のラベル付けの不整合
B. トレーニングセットのデータ不足により、モデルが地域パターンを学習できない。
C. 顧客需要の最近の変化によるモデルのずれ
D. モデルの過学習により、売上記録が誤って表示される
正解: **(**正解を表示します**)**
このシナリオは、「データ不足」または「過小代表バイアス」の問題を示しています。モデルが主に都市部のデータでトレーニングされている場合、農村地域の特有の経済状況や競争環境を理解するのに十分な情報が得られません。その結果、農村地域に遭遇した際に、限られたデータに基づいて「推測」しているため、不規則または極端な推奨事項（過剰な割引など）を提示する可能性があります。AAIA™マニュアルによると、すべての人口統計学的または地理的サブグループにわたって「データの代表性」を確保することは、トレーニングにお

ける重要なステップです。バランスの取れたデータセットがないと、モデルはすべての運用環境に正しく一般化できず、重大な財務損失と運用上の不安定性につながります。

質問: **172**
ある組織が、回避攻撃に対して脆弱なAIベースの画像認識システムを導入しました。システムがこれらの回避攻撃を確実に軽減するために、次のうちどの方法が最も効果的でしょうか？
A. 静的ルールに基づく入力フィルタリングと検証
B. 厳格なモデル精度評価基準
C. モデルアンサンブルの実装
D. 敵対的トレーニングと定期的なバイアスレビュー
正解: **D** (コメントを発表する)
回避攻撃とは、攻撃者が入力データ（画像に微妙なノイズを加えるなど）を改変して、モデルを騙して誤分類させる攻撃のことです。AAIA™ マニュアルでは、「敵対的トレーニング」を主要な防御策として挙げています。これは、トレーニング段階で意図的に敵対的サンプルにモデルをさらすことで、モデルの堅牢性と回復力を向上させるものです。これにより、モデルは悪意のある入力に関連するパターンを学習できます。静的フィルタリング（オプション A）とアンサンブル（オプション C）は防御層を提供できますが、高度な攻撃によって回避されることがよくあります。定期的なバイアスレビューは、アルゴリズムの弱点を悪用するように設計された入力を含め、すべての入力に対してモデルの意思決定が公平かつ一貫していることをさらに保証します。

質問: **173**
AIモデルが偏りなく動作していることを確認するために、以下のうちどれをレビューすることが最も重要ですか？
A. AIトレーニングデータ
B. AI開発環境
C. AIモデルの適応性
D. AIモデルの温度
正解: (正解を表示します)
AIモデルにおけるバイアスは、トレーニングデータを通じて最も一般的に発生します。AAIATMの学習ガイドでは、公平性を確保するためには、監査担当者と開発者が、モデルのトレーニングに使用されるデータの多様性、代表性、および品質を評価する必要があると強調しています。
「AIにおけるバイアスの最大の原因は、学習データにあります。このデータを精査し監査することは、出力が特定のグループに不均衡な影響を与えたり、結果を歪めたりしないようにするために不可欠です。」

質問: **174**

ある組織が、融資申請の評価を支援するために大規模言語モデル（LLM）を使用しているが、使用されている訓練データが不完全であることがわかっている。以下のうち、最も大きな関連リスクはどれか？
A. 不当な融資決定
B. 融資承認の遅延
C. 顧客満足度の低下
D. 申請処理の手動化
正解: **(**正解を表示します**)**
トレーニングデータが不完全な場合、特定の申請者タイプ、商品、またはシナリオが過小評価されることがよくあります。信用供与や融資においては、これは通常、体系的な偏りにつながります。つまり、一部のグループはより豊富な過去のデータに基づいて評価される一方で、他のグループは乏しい、あるいは代表性のない情報に基づいて評価されることになります。したがって、最も大きなリスクは不公平な融資決定（A）であり、これは不当な拒否、不適切な価格設定、または一貫性のないリスク評価として現れる可能性があります。
遅延（B）、顧客満足度の低下（C）、手作業の増加（D）などが発生する可能性はあるものの、これらは二次的な業務上の問題である。AAIAは、金融サービスにおける中心的なリスクとして、公平性、差別、規制遵守、評判への影響を挙げている。不完全なデータは公平性を直接的に損ない、融資規制や社内リスク許容度に違反する可能性がある。
参考文献：
ISACA、AAIA試験内容概要 - ドメイン1：AIガバナンスとリスク（公平性や差別的な結果を含むリスクカテゴリ）。
ISACAのAI倫理に関するコンテンツ：意思決定システムにおけるデータの完全性と代表性について。

質問: **175**
IS監査担当者は、AIモデルがテストデータよりも訓練データにおいて著しく優れた結果を達成したと指摘している。
IS監査担当者は、モデルに関して以下のどの問題点を特定しましたか？
A. アンダーフィッティング
B. 過学習
C. 一般化
D. バイアス
正解: **B (**コメントを発表する**)**
過学習とは、モデルが訓練データに対しては非常に優れた性能を発揮するものの、未知のデータに対しては性能が低下する現象であり、モデルが効果的に汎化するのではなく、訓練データセットに特有のパターンを学習してしまったことを示しています。AAIA™学習ガイドでは、過学習はモデルの信頼性に影響を与える一般的な問題として挙げられています。

過学習は、モデルの実世界への適用可能性を制限します。これは、訓練データへの過剰な適合と、新しい多様な入力に対する性能の低下を反映しています。」過小適合（A）は、訓練データとテストデータの両方で性能の低下を招きます。汎化（C）は望ましい状態であり、バイアス（D）は別の問題です。したがって、Bが正解です。
参考資料：ISACA Advanced in AI Audit™ (AAIA™) 学習ガイド、セクション：「AIの運用とパフォーマンス」、サブセクション：「過学習、過小学習、および汎化」

質問: **176**
即時インジェクション攻撃に対するインシデント管理手順の一環として、以下のどの手法が最も効果的でしょうか？
A. AIモデルを微調整します。
B. テキストのコードのような構造をスキャンします。
C. 不正利用のプロンプトをサニタイズするために、入力検証を導入します。
D. プロンプトに過剰な特殊文字がないか監視します。
正解: **(**正解を表示します**)**
プロンプトインジェクション攻撃とは、システム命令の上書き、データの漏洩、または有害な動作を引き起こすことを目的とした、悪意を持って作成された入力を用いる攻撃です。インシデント管理と連携した最も効果的な対策は、堅牢な入力検証とサニタイズ（C）を導入することです。これには、潜在的に悪意のあるコンテンツがモデルに到達する前に検出して無効化するように設計されたルールとフィルタが含まれます。AAIAによるAIの脅威と脆弱性に関する記事では、生成型AIシステムにおける入力検証と安全なプロンプト処理の重要性が強調されています。

質問: **177**
ある組織が、顧客が好みを入力すると最適な商品を提案するAIチャットシステムを導入しました。システムが顧客を不快にさせる可能性のある提案を行うリスクを軽減するための最善の方法は次のうちどれですか？
A. データセットが公平かつ偏りのないものとなるよう、トレーニングデータの量を増やします。
B. さまざまなシナリオでテストを実施し、出力が許容範囲内であることを確認します。
C. AIサーバーの継続的な監視を実施し、技術的なパフォーマンスの異常を検出します。
D. 未知のリスクを特定するために脅威分析を実施する。
正解: **(**正解を表示します**)**
ここで述べられているリスクは、顧客向けの提案が不適切、無神経、または攻撃的である可能性があるということです。最善の対策は、エッジケース、人口統計学的変動、およびデリケートな状況を含む多様なシナリオ（B）のテストを実施し、出力が許容可能なビジネス、倫理、および顧客体験の基準内に収まっていることを確認することです。AAIAは、特に推奨事項が顧客とのやり取りに直接影響を与える場合、シナリオベースのテストと公平性／影響評価を重要な実践として強調しています。

データ量の増加（A）は、公平性や機密性を保証するものではありません。サーバーの監視（C）は技術的な健全性に焦点を当てており、コンテンツの適切性には対応していません。脅威分析（D）はセキュリティにとって重要ですが、モデル出力の感情的または倫理的な影響に直接対処するものではありません。したがって、構造化された多様なシナリオテストが、最も的を絞った効果的なアプローチとなります。
参考文献：
ISACA、AAIA試験内容概要 - ドメイン2およびドメイン5：テスト手法、倫理およびユーザーへの影響に関する考慮事項。
ISACAのAIに関するガイダンス：公平性、適切性、およびユーザーへの影響を考慮したシナリオテストについて。

質問: **178**
組織がリアルタイム予測のためにパブリッククラウド環境に機械学習モデルを導入する場合、以下のうちどれが最も大きなリスクとなるでしょうか？
A. クラウドプロバイダーの従業員はAIスキルが限られている
B. AIモデルの監査証跡が包括的に文書化されていない
C. サービスレベル契約（SLA）には、ネットワーク遅延および推論保証は含まれません。
D. クラウドプロバイダーは倫理的なAIガバナンスフレームワークを採用していません
正解: **(**正解を表示します**)**
リアルタイム予測環境（例えば、不正検出、医療トリアージ、自動車リスク評価など）では、レイテンシと推論速度が安全性、精度、およびビジネスパフォーマンスに直接影響します。SLAに遅延に関する保証が含まれていない場合、モデルは予測を時間通りに提供できず、以下のような事態が発生する可能性があります。
誤った、または遅れた決定
取引の失敗
時間的制約のある使用事例における安全上のインシデント
規制対象分野における法令違反

質問: **179**
不均衡なデータセットにおけるモデルのパフォーマンスを測定するための最適な主要業績評価指標（KPI）は次のうちどれですか？
A. F1スコア
B. 精度
C. リコール
D. エラー率
正解: **A (**コメントを発表する**)**
データセットが不均衡な場合、標準的な「精度」や「エラー率」は誤解を招く可能性があります（例えば、トランザクションの99%が正当な場合、毎回「正当」と予測するモデルは99%の精度を持ちますが、不正検出には役に立ちません）。「F1スコア」は、適合率と再現率の調和平均であり、偽陽性と偽陰性の両方を考慮したバランスの取れた指標です。これは、モデル

が少数派クラスをどれだけうまく処理できるかを評価するための業界標準のKPIです。適合率と再現率はそれぞれに価値がありますが、F1スコアは、偏った環境におけるモデルの有効性を包括的に示す単一の指標となります。

質問: **180**
AIシステムの透明性を監査する際、モデルの意思決定プロセスを理解する上で最も効果的な方法は次のうちどれでしょうか？
A. トレーニングデータセットの多様性を評価する
B. 使用されているアルゴリズムの複雑さを分析する
C. モデルの計算コストの評価
D. AI出力の説明可能性の検証
正解: **D** (コメントを発表する)
AIシステムにおける透明性は、信頼性、説明責任、倫理遵守を確保するための重要な要件である。
ISACA AAIA™学習ガイドの「AIガバナンスとリスク管理」のセクションによると、AIシステムの意思決定プロセスを理解することは、説明可能性の原則に該当する。
説明可能性とは、観察者がAIシステムの内部構造や出力の背後にある論理をどの程度理解できるかを示す指標である。
「AI出力の説明可能性を検証することで、監査担当者や利害関係者は、モデルの決定が解釈可能で正当化できるかどうかを判断できます。高い透明性とは、利害関係者が決定がどのように、そしてなぜ行われたかを追跡できることを意味します。」アルゴリズムの複雑さや計算コストは技術的な考慮事項ではありますが、意思決定の透明性の監査を直接促進するものではありません。同様に、トレーニングデータの多様性はバイアスの低減に不可欠ですが、決定がどのように導き出されたかを説明するものではありません。したがって、オプションDが監査の透明性に最も合致しています。
参考資料：ISACA Advanced in AI Audit™ (AAIA™) 学習ガイド、セクション：「AIガバナンスとリスク管理」、サブセクション：「透明性と説明可能性」

質問: **181**
食品配達サービスがAIモデルを利用する場合、どのユースケースが組織にとって倫理的なリスクをもたらすでしょうか？
A. 時間、コスト、配送距離、顧客満足度などの指標を関連付け、標準以下のサービスを受けた顧客にクーポンを発行する
B. ドライバーの雇用継続および解雇の決定は、業界ベンチマークと比較した総労働時間あたりの配達済み注文数に基づいて行う。
C. 食品の調理時間と配達時間の合計を業界ベンチマークと比較し、各レストランの主要業績指標とリスク指標を設定する。
D. サービス速度と食品品質に関する顧客サービス指標を用いて、顧客維持率を予測し、収益を予測する。

正解: **B** (コメントを発表する)

有効的な**AAIA**問題集はJPNTest.com提供され、**AAIA**試験に合格することに役に立ちます！JPNTest.comは今最新**AAIA**試験問題集を提供します。JPNTest.com AAIA試験問題集はもう更新されました。ここで**AAIA**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/AAIA-mondaishu　**328**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **182**
組織が成熟したMLOpsの実践を行っていることを示す最良の指標は次のうちどれですか？
A. モデルはパイプラインを介さずにデータサイエンティストによって直接デプロイされます
B. テスト、検証、監視、ロールバック機能を備えた自動化されたCI/CDパイプライン
C. すべてのモデルは年に一度手動で再学習されます
D. モデルドキュメントはオプションです
正解: **B** (コメントを発表する)
成熟したMLOpsは、自動テスト、検証ゲート、継続的な監視、ロールバックメカニズムをデプロイメントパイプラインに統合し、機械学習に適用されるDevOpsの規律を反映させる。

質問: **183**
次のうち、AIモデルの出力におけるモデルドリフトや予期せぬ変化を最も効果的に検出できるのはどれですか？
A. AI構成の標準化
B. 異常監視
C. AIモデルのドキュメントレビュー
D. AIモデルの再学習
正解: (正解を表示します)
異常監視は、入力データやモデル出力における不規則性や逸脱を検出します。これらはモデルのドリフトを示す重要な指標です。AAIATM学習ガイドによると、継続的な異常検出は、データ環境の変化によってモデルが期待どおりに機能しなくなった時期を特定する最も効果的な方法の1つです。
出力異常を監視することで、モデルのドリフトを早期に特定できます。この積極的なアプローチにより、組織はパフォーマンスが著しく低下する前にモデルを再学習または調整することが可能になります。」

質問: **184**
風力タービン発電機の故障を予測するために機械学習（ML）モデルを使用する場合、どのモデル評価指標を最優先すべきでしょうか？

A. 精度
B. リコール
C. 精度
D. 特異性
正解: **(**正解を表示します**)**

質問: **185**
金融機関の取引処理システムの監査を実施するためのサンプルを選択する際に、AIツールを使用する際に優先的に考慮すべき事項は次のうちどれですか？
A. サンプリングプロセスの透明性
B. 大量のデータを処理する能力
C. サンプル生成速度
D. 過去の監査における実績
正解: **(**正解を表示します**)**
監査においては、サンプリングの透明性が、サンプルが公平かつ偏りがなく、監査目的に合致していることを示すために不可欠です。AIツールが金融取引のテスト用サンプルを選択する場合、監査人は、特に経営陣、規制当局、および外部の利害関係者に対して、サンプルがどのように生成されたかを説明し、擁護できなければなりません。オプションAは、AAIAが重視する監査計画、サンプリング手法、およびAI監査証拠を直接的にサポートします。

質問: **186**
ある医療機関は、AIモデルを用いて患者データを分析し、診断に関する推奨事項を提供している。
モデルの予測に関連するデータドリフトを最も効果的に検出できるのは、次のうちどれですか？
A. 入力された患者データの分布をトレーニングデータセットと比較する
B. 医療従事者がAIモデルの推奨事項を修正できるように、オーバーライドを適用する。
C. 最新の患者データとの整合性を確保するため、定期的にモデルの再トレーニングを実施する。
D. 敵対的テストを用いて、モデルの予測をストレステストするシナリオをシミュレートする
正解: **(**正解を表示します**)**
データドリフトの検出は、AIモデルの信頼性と精度を維持する上で非常に重要であり、特に医療のような動的な環境では、患者集団やデータ特性が時間とともに変化する可能性があるため、なおさら重要である。
ISACA Advanced in AI Audit™ (AAIA™) 学習ガイドによると、データドリフトとは、入力データの統計的特性が、モデルが最初にトレーニングされたデータと比較して変化することを指します。
データドリフトが検出されない場合、モデルのパフォーマンスが低下し、誤った予測につながる可能性があります。

データドリフトを検出する最も効果的な方法は、入力データ（本番データ）の統計分布をトレーニングデータセットの統計分布と継続的に比較することです。これにより、組織はデータパターンのずれを特定でき、AIモデルの予測がもはや有効または最適ではない可能性を示す早期の兆候を捉えることができます。
AAIA™学習ガイドの「AIモデルの監視とメンテナンス」の項に記載されているとおりです。「入力データの分布の変化をモデルのトレーニングデータと比較して監視することは、データドリフトを特定する上で不可欠なステップです。統計的テストと視覚化は、監査担当者やAIオペレーターが、基となるデータ特性が変化した時期を検知し、さらなる調査や再トレーニングの必要性を判断するのに役立ちます。」モデルの再トレーニング（オプションC）や敵対的テスト（オプションD）などのオプションは、継続的なパフォーマンスと堅牢性にとって価値がありますが、データドリフトを本質的に検出するものではなく、既存の問題に対応したり、ストレステストを実施したりするものです。オーバーライドの適用（オプションB）は、ヒューマン・イン・ザ・ループの安全策であり、ドリフト検出の方法ではありません。
参考資料：ISACA Advanced in AI Audit™ (AAIA™) 学習ガイド、セクション：「AIモデルの監視と保守」、サブセクション：「データドリフトの検出と管理」

質問: **187**
IS監査担当者がAIモデルのスコアカードを分析した結果、トレーニングデータに偏りがあることがわかった。
リスクを軽減するための最適な推奨事項は次のうちどれですか？
A. 階層化された訓練/検証分割を用いたクラス加重損失を使用します。
B. 誤分類の予想コストを用いて判定閾値を調整する。
C. 検証時のF1スコアが最大になるように決定閾値を最適化します。
D. 早期停止機能を備えたモデルの容量を増やす。
正解: **A** (コメントを発表する)
データ不均衡（あるクラスが他のクラスを著しく上回る場合）は、少数派クラスに対する性能が低い偏ったモデルにつながります。ISACA AAIATM マニュアルでは、「クラス加重損失」は、少数派サンプルを誤分類した場合にモデルにペナルティを課し、学習プロセスを効果的に「バランスさせる」ための積極的な技術的制御であると示唆しています。層別分割により、各トレーニングセットと検証セットが元のデータと同じクラス比率を維持することが保証され、テスト段階でモデルが少数派ケースを「認識できない」事態を防ぎます。

質問: **188**
高リスクなAIシステムの開発と設計を支援するための最良の方法は、次のうちどれですか？
A. ユーザー向けにデータプライバシーに関する定期的な研修を実施する。
B. AIシステムのデータを定期的に安全なオフサイトの場所にバックアップしてください。
C. AIシステムにアクセスするすべてのユーザーに対して多要素認証（MFA）を実装する。

D. 信頼できるデータセットが利用可能であることを確認する。
正解: **(**正解を表示します**)**

質問: **189**
AIシステムを用いた適切なデータ管理を確保するために、検証すべき最も重要な制御項目はどれですか？
A. データガバナンスの枠組みが確立されました。
B. 適切なデータ指標が開発されました。
C. データインベントリが決定されました。
D. データは感度に応じてラベル付けされています。
正解: **A (**コメントを発表する**)**
ISACA AAIA™学習ガイドによると、「データガバナンスフレームワーク」は基盤となる統制です。これは、データライフサイクル全体を管理するために必要なポリシー、役割（管理者所有者）、および標準を提供します。フレームワークがない場合、インベントリ作成（オプションC）やラベル付け（オプションD）などの活動は場当たり的になり、説明責任が欠如します。正式なフレームワークは、データ管理が一貫性があり、プライバシー法に準拠し、組織のリスク許容度と整合していることを保証します。これは、他のすべてのデータ品質およびセキュリティ指標を意味のあるものにし、強制力を持たせる「基盤となる」統制です。

質問: **190**
AIモデルのトレーニングに使用されるデータに関連する倫理的リスクを評価する際に、最も重要な考慮事項は次のうちどれですか？
A. 多様な出力を生成する能力
B. トレーニングデータの感度と出所
C. モデル更新の頻度
D. トレーニングデータのクリーニングおよび検証方法
正解: **B (**コメントを発表する**)**
倫理的リスクは、使用されるデータの性質から始まります。トレーニングデータ（オプションB）の機密性と出所によって、モデルがプライバシー侵害、過去の偏見の永続化、または適切な同意なしに収集されたデータの使用といったリスクを抱えるかどうかが決まります。AAIAは、倫理的なAIにおいて、データの出所、データの機密性、および処理の合法性を中核的な要素として挙げています。健康状態、民族性、性別、経済状況などの機密性の高い属性を含むトレーニングデータは、法令遵守と倫理的影響について慎重に検討する必要があります。

質問: **191**
IS監査担当者が、ベンダーからのメールに埋め込まれた「プロンプトインジェクション」を検出しました。このメールは、テキストを隠すために不可視フォントを使用していました。次のうち、最も適切な対策はどれですか？

A. 温度を下げることで、AI モデルが注射に従う可能性を低くします。
B. AIモデルに、見えないテキストを無視するように指示を追加します。
C. 取り込み前に目に見えないテキストを削除するテキストサニタイズを実装します。
D. フォントをデフォルトに変更するテキストサニタイズを実装します。
正解: **(**正解を表示します**)**
これは「隠しテキスト」攻撃であり、攻撃者は人間には見えないが機械が処理できる命令を埋め込むことでLLMを欺きます。最も効果的な「インシデント管理」対策は「テキストサニタイズ」であり、テキストがAIに送信される前に、目に見えない書式設定、隠しHTMLタグ、またはゼロ幅文字を具体的に削除します。命令を追加する（オプションB）方法は、プロンプトインジェクションが以前の命令を「上書き」するように設計されているため、信頼性に欠けます。温度を下げる（オプションA）方法は創造性を低下させますが、モデルが明確ではあるものの隠された命令に従うことを止めることはできません。

質問: **192**
監査計画にAIを使用する際に最も大きなリスクとなるのは、次のうちどれですか？
A. 計画コストの増加
B. スコープクリープ
C. データが不完全です
D. 知識が限られている
正解: **(**正解を表示します**)**
AIを活用した監査計画の文脈において、AAIATM学習ガイドは、不完全または不正確なデータが最も重要なリスクであると指摘しています。AIツールに入力されるデータが欠落していたり、古くなっていたり、矛盾していたりすると、リスクの優先順位付けやコントロールテストに関するモデルの提案は不正確なものとなります。
「AIツールを活用した監査計画の有効性は、基となるデータの質に左右されます。データが不完全な場合、リスク評価が不正確になったり、監査リソースの配分が誤ったりして、監査の有効性が損なわれる可能性があります。」プロジェクト管理において、スコープの拡大やコスト増はよくある懸念事項であり、AIの知識不足はトレーニングによって軽減できますが、監査計画の成果物の妥当性に直接影響を与えるのは、データの不完全性だけです。

質問: **193**
監査チームが監査報告書の作成に生成型AIを利用する場合、以下のうちどれが最も大きな懸念事項でしょうか？
A. 報告書には古い情報が反映されている可能性が高いです。
B. 報告書には幻覚による誤った記述が含まれている可能性があります。
C. 報告書は、以前の監査結果とは異なる書式を使用している可能性があります。
D. 報告書では、監査上の問題について一般的な表現が使われる傾向があるかもしれません。
正解: **(**正解を表示します**)**

最大の懸念は、生成モデルが誤った事実や結論（選択肢B）を生み出す可能性があることです。監査の文脈では、このような誤った予測は、統制の有効性に関する虚偽の記述、リスクの誤報告、または証拠の不正確な要約につながる可能性があります。
AAIAは、監査人は職業的懐疑心を維持し、AIが生成したコンテンツを検証する必要があると強調している。誤った記述は、監査の信頼性、規制遵守、組織の意思決定を損なうため、重大なリスクとなる。

質問: **194**
大規模言語モデル（LLM）チャットボットによる機密情報の漏洩を防ぐ最善の方法は次のとおりです。
A. 手動監視
B. アクセス制御
C. データサニタイズ
D. データマスキング
正解: **(**正解を表示します**)**
大規模言語モデル（LLM）は、適切に管理されない場合、機密情報を記憶し、意図せず漏洩する能力を持っています。AAIATM学習ガイドによると、データマスキングは、トレーニングやインタラクション中にデータの機密部分を隠蔽または置換することで、個人識別情報（PII）や機密コンテンツの漏洩を防ぐ重要な技術です。
データマスキングは、LLM（学習モデル）に使用されるトレーニングデータに実際の機密識別子が含まれないようにします。サニタイズとは異なり、マスキングはデータを修正して有用性を維持しながら、情報漏洩のリスクを排除します。手動による監視とアクセス制御は補助的なセキュリティ対策であり、データサニタイズはコンテンツの削除に役立ちますが、データの構造を維持できない場合があります。データマスキングは、最も積極的かつ技術的に堅牢なソリューションを提供します。

質問: **195**
AIライフサイクルにおいて、エッジケースを評価するのに最も適切な段階は次のうちどれですか？
A. 計画と設計
B. 操作と監視
C. 収集と処理
D. テストと検証
正解: **(**正解を表示します**)**
エッジケース（AIが予測不能な動作をする可能性のある、まれではあるが重大なシナリオ）の評価は、テストおよび検証段階（D）で実施する必要があります。この段階は、極端な入力や異常な入力をシミュレートし、負荷がかかった状態でのパフォーマンスを検証し、展開前に堅牢性と安全性を確保するように設計されています。AAIAは、エッジケース評価を含む堅牢性テストが、AIソリューションの重要なテスト手法であることを強調しています。

計画（A）とデータ収集（C）は入力データを準備するものの、モデルの動作評価は行いません。運用と監視（B）は後から問題を検出する可能性がありますが、リスクを軽減するためには、展開前にエッジケースのテストを実施する必要があります。
参考文献：
ISACA、AAIA試験内容概要 - ドメイン2：AIソリューションのテスト手法（エッジケース、堅牢性テスト）。

質問: **196**
以下のテスト手法のうち、組織のデータガバナンスプログラムがAIモデルのトレーニングと展開におけるデータ品質と整合性を効果的に保証しているかどうかを最も適切に検証できるのはどれですか？
A. AIモデルの不具合による影響を評価するための事業影響分析（BIA）を実施する
B. 組織のAIソフトウェア開発ライフサイクル文書のレビュー
C. モデルの脆弱性を特定するための侵入テストを実施する
D. データソースのトレーサビリティを検証するためのデータ系統の評価
正解: **(**正解を表示します**)**
データリネージを評価することで、データのライフサイクル全体における発生源、流れ、および変換に関する洞察が得られ、これはデータガバナンスの検証に不可欠です。AAIA™学習ガイドでは、AIモデルのトレーニングに使用されるデータの正確性、一貫性、および信頼性を確保するために、データリネージが不可欠であると述べています。
「データソースのトレーサビリティは、効果的なデータガバナンスの中核をなす原則です。データリネージの検証は、データ品質を保証し、不正な変更を防止し、監査可能性を維持します。」BIA（A）は影響に焦点を当てており、データ品質には焦点を当てていません。SDLC（B）のレビューは広範であり、データ固有のリスクを明確に示さない可能性があります。侵入テスト（C）はセキュリティを対象としており、ガバナンスには焦点を当てていません。したがって、Dが最良の方法です。
参考資料：ISACA Advanced in AI Audit™ (AAIA™) 学習ガイド、セクション：「AIガバナンスとリスク管理」、サブセクション：「データ品質、整合性、およびガバナンスの実践」

有効的な**AAIA**問題集はJPNTest.com提供され、**AAIA**試験に合格することに役に立ちます！JPNTest.comは今最新**AAIA**試験問題集を提供します。JPNTest.com AAIA試験問題集はもう更新されました。ここで**AAIA**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/AAIA-mondaishu　328問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **197**
IS監査担当者は、複雑な問題を含む監査の報告を迅速化したいと考えています。監査担当者が生成型AIを使用する最も効果的な方法は次のうちどれでしょうか？

A. 経営陣からの新たな情報に基づき、監査の背景情報および範囲情報を修正する
B. 監査所見を正確な表現で記述し、監査結論を修正する
C. 経営行動計画の最終会議で議論された行動項目を作成する
D. 詳細な調査結果と監査範囲に基づいて、エグゼクティブサマリーの草案を作成する。
正解: **D** (コメントを発表する)

質問: **198**
従来の監査方法と比較して、AI監査技術を使用する最大の利点は、AI監査技術が以下のことを可能にする点です。
A. 人間の介入の必要性を排除する。
B. 複雑なデータパターンを識別する。
C. 規制を完全に遵守すること。
D. データバイアスを大幅に低減します。
正解: (正解を表示します)

質問: **199**
ある組織が、自社の月次データに基づいて学習させたAIモデルを開発しました。データドリフトを回避するための最適な検証方法は次のうちどれでしょうか？
A. 10分割交差検証
B. 顧客IDでグループ化して分割
C. 時系列
D. 全月にわたってランダムに分割
正解: **C** (コメントを発表する)
月次データや時系列データを扱う場合、標準的なランダム分割（オプションD）や交差検証（オプションA）では、「時間的リーク」が発生する可能性があります。これは、モデルが意図せず将来のデータから学習して過去を予測してしまう現象です。ISACA AAIATMの原則によれば、時系列データには「時系列」検証が最も適切な方法です。この方法では、特定の期間（例1:〜0ヶ月目）でモデルをトレーニングし、次の期間（例1:1ヶ月目）でテストします。このアプローチは、モデルが本番環境でどのように動作するかを正確に反映し、季節的な傾向や顧客行動の長期的な変化によってモデルの精度が時間とともに低下する時期を特定できるため、データドリフトの検出に不可欠です。

質問: **200**
IS監査担当者が、自律的な脅威検出とインシデント対応にエージェント型AIを使用するサイバーセキュリティシステムを評価しています。監査担当者が考慮すべき最も重要な事項は次のうちどれですか？
A. エージェントは複数のシステム間で動作するため、ネットワークの拡張が必要になる場合があります。

B. エージェントがデータを自律的に処理するため、アナリストの介入の必要性が軽減されます。
C. エージェントの監査ログは、従来のログよりも長くなります。
D. エージェントは、業務運営を妨害する可能性のある自動アクションを実行する場合があります。
正解: **(**正解を表示します**)**
「エージェント型AI」は、単なる検出にとどまらず、サーバーのシャットダウンなどの行動を自律的に実行できる。
最大の危険は、AIが正当ではあるものの通常とは異なる業務活動を脅威と誤認し、「キルスイッチ」を作動させ、大規模かつ予期せぬシステム停止を引き起こす可能性があることです。これは、運用面および可用性において重大なリスクとなります。監査担当者は、影響の大きい操作に対して「ガードレール」または「ヒューマン・イン・ザ・ループ」が確保されていることを確認する必要があります。介入の削減（オプションB）は利点である一方で、監査担当者がガバナンスと統制の評価を通じて軽減しなければならないリスクの源泉でもあります。

質問: **201**
AIモデルの出力におけるバイアスを効果的に制御するための最良の方法は、次のうちどれですか？
A. さまざまな人口統計グループにおける精度範囲は類似しています。
B. 組織のAIポリシーには、公平性に関する明確な定義が含まれています。
C. モデルのトレーニングは、現実世界の人間の意思決定を含むデータに限定されます。
D. モデル開発プロセスの技術的な詳細は透明性があります。
正解: **(**正解を表示します**)**
バイアス制御の最も客観的な証拠は「パフォーマンスの均一性」です。精度、適合率、再現率が「さまざまな人口統計グループ間で類似している」場合、モデルがすべてのユーザーに対して公平に機能していることを示します。ポリシー定義（オプションB）を持つことは優れたガバナンスですが、モデルが実際に公平であることを証明するものではありません。「現実世界の人間の意思決定」（オプションC）にトレーニングを限定すると、過去の人間の差別を自動化するだけであるため、バイアスが生じることがよくあります。透明性（オプションD）は監査に必要ですが、それだけではモデルのバイアスを防ぐことはできません。

有効的な**AAIA**問題集はJPNTest.com提供され、**AAIA**試験に合格することに役に立ちます！JPNTest.comは今最新**AAIA**試験問題集を提供します。JPNTest.com AAIA試験問題集はもう更新されました。ここで**AAIA**問題集のテストエンジンを手に入れます。最新版

のアクセス、https://www.jpntest.com/shiken/AAIA-mondaishu　328問、３０%ディスカウント、特別な割引コード: **JPNshiken**」