ISACA.AAIA.v2026-06-08.q124

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：	124
バージョン：	v2026-06-08
ページの閲覧量：	104
問題集の閲覧量：	1310

https://www.jpnshiken.com/shiken/ISACA.AAIA.v2026-06-08.q124.html

質問: **1**
機械学習（ML）ソリューションの監査を行う際、誤検出を最も適切に評価するには、以下のレベルを検証する必要があります。
A. 完全性
B. 精度
C. リコール
D. 精度
正解: **(**正解を表示します**)**

質問: **2**
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: **3**
ある銀行は、動画を用いた顧客確認（KYC）プロセスを採用しています。サイバー犯罪者は、ディープフェイク技術を用いて銀行の顧客になりすますことで、このプロセスを悪用しています。銀行がこのリスクを軽減するために、次のうちどれが最適な対策でしょうか？
A. ビデオ認証におけるAIベースの生体検知の活用
B. 本人確認および住所確認のため、追加の身分証明書および住所証明書類を要求します。
C. すべての顧客データと通信を暗号化します
D. ビデオ認証プロセスの使用を中止する
正解: **A** (コメントを発表する)

質問: **4**
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. 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
B. 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
C. 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。
D. 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。

正解: **(**正解を表示します**)**

質問: **5**
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: **(**正解を表示します**)**
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: **6**
投資機関のAI搭載ソフトウェアの監査中に、情報システム監査担当者が潜在的なセキュリティリスクを特定しました。組織のデータを生成型AIツールに持ち出すことに関連する最大のリスクは何ですか？
A. AIが生成した知見への過度の依存
B. 事業の中断の可能性
C. 偏ったAIモデル出力によるデータ汚染
D. 不正なデータ開示
正解: **D (**コメントを発表する**)**

質問: **7**

エンドユーザーがAIツールを利用できるようにする前に、組織にとって最も重要な行動は次のうちどれですか？
A. 災害復旧計画（DRP）への影響を判断する。
B. AIの使用を含むサイバーセキュリティ保険条項が盛り込まれていることを確認してください。
C. 適切な使用に関するガイドラインを含むAIポリシーを策定する。
D. ベースラインのパフォーマンス指標を導入する。
正解: **(**正解を表示します**)**

質問: **8**
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. 個人の権利の保護とシステムが整合するようにするため
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. モデル内の潜在的なデータドリフトを特定し、軽減する
D. システムの精度と性能を向上させる
正解: **(**正解を表示します**)**

質問: **9**
製品レビューの感情分析を行う機械学習（ML）モデルが利用するデータを、競合他社が改ざんするリスクを軽減するのに役立つ対策は、次のうちどれですか？
A. ソーシャルメディアの投稿から製品レビューを取得するピアレビューコード
B. マーケティング会社を雇い、顧客に商品レビューを依頼するリンクをテキストメッセージで送信し、金銭的な報酬を支払う。
C. 顧客が商品レビューを投稿する前に、アカウントへのアクセス認証を要求する
D. モデル開発者によるオーバーサンプリングを用いた、不均衡な製品レビューデータセットの拡張
正解: **(**正解を表示します**)**

質問: **10**
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: **C (**コメントを発表する**)**
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: **11**
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: **12**
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: **13**
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、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であるデータポイ

ズニング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: **14**
既製のAIモデルを使用する場合、組織がベンダー管理に取り組む上で最も適切な方法は次のうちどれですか？
A. 市場調査と比較のために、最低3社の見積もりを取得してください。
B. モデルの更新とサポートに関する責任と明確な条件を確立する。
C. 世界的に認められた認証を取得しているベンダーのモデルのみを使用してください。
D. 情報セキュリティ部門による契約内容の審査が済んでいる場合にのみ、そのベンダーを利用してください。
正解: **(**正解を表示します**)**
組織が既製のAIモデルを活用する場合、運用上の信頼性、コンプライアンス、および長期的なサポートを確保するためには、効果的なベンダー管理が不可欠です。ISACA Advanced in AI Audit™ (AAIA™) 学習ガイドでは、「継続的なモデルの更新、保守、サポート、およびインシデント対応に関する責任について明確な契約条件を確立することが、サードパーティAIのリスク管理に不可欠である」と強調しています。更新とサポートに関する役割と期待を明確に定義することで（オプションB）、組織は、未解決の脆弱性、時代遅れのモデル、またはインシデントやシステム障害発生時の対応策の不明確さといったリスクを軽減できます。このアプローチは、継続的なリスク管理をサポートし、モデルのライフサイクル全体を通して、両当事者がそれぞれの義務を理解することを保証します。
市場調査、ベンダーの認定、情報セキュリティ部門による契約審査は重要なデューデリジェンスの手順ではあるものの、AIソリューションの効果的なガバナンスと持続的な運用に不可欠な、ベンダーの継続的な責任の明確化というニーズに直接対応するものではない。
参考資料：ISACA Advanced in AI Audit™ (AAIA™) 学習ガイド、セクション：「AIシステムのベンダー管理」、サブセクション：「サードパーティAIのリスクと契約上の義務」

質問: **15**
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。
C. 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出力に反映します。
D. 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。
正解: **(**正解を表示します**)**

質問: **16**
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: **(**正解を表示します**)**
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　275問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **17**
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. 業界におけるAIシステムの未成熟

B. AIシステム保守に関連する費用
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**)**

質問: **18**
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: **(**正解を表示します**)**
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。
敵対的テストの結果は、インシデント対応計画（A）、KRIの定義（B）、またはセキュリティ意識向上（C）に役立つ可能性があるものの、これらは二次的な利点です。AAIAのAI脅威と脆弱性に関する解説では、AI特有のリスクへの曝露に直接対処する制御検証およびギャップ特定メカニズムとして、敵対的テストを重視しています。
参考文献：
ISACA、AAIA試験内容概要 - ドメイン1およびドメイン2：AIに特有の脅威と脆弱性、AIソリューションのテスト手法。
ISACAによる敵対的テストおよびAIセキュリティ態勢評価に関するガイダンス。

質問: **19**
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: **C (**コメントを発表する**)**
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、パフォーマンスの低下や少数派クラスへの不公平な扱いにつながる可能性があります。リスクの高いアプリケーション（不正検出、信用スコアリング、医療診断など）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強調し、軽減策（リサンプリング、重み付け、閾値調整）の重要性を説いています。
データドリフト（A）とは、時間経過に伴うデータ分布の変化を指しますが、これは時間経過とは無関係です。データ品質（B）はより広範な概念であり、不均衡の影響を受ける場合と受けない場合があります。過学習（D）はリスクですが、クラスの不均衡は、過学習単独よりも公平性と代表性に関する懸念をより直接的に引き起こします。したがって、クラスの不均衡から生じるバイアスが、監査人の主要な懸念事項となります。
参考文献：
ISACA、AAIA試験内容概要 - ドメイン2：AIに特化したデータ管理（データバランス、バイアスリスク）。
ISACAのAI倫理およびモデルリスクに関するガイダンスでは、階級格差と公平性について議論されている。

質問: **20**
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
* 即時注射
* 不正なモデル操作 AAIA は、従来の IT 脅威モデリングでは十分に対処できない AI 固有のセキュリティリスクを予測および軽減するために AI 脅威モデリングが不可欠であることを強調しています。オプション C (規制遵守) は二次的な利点です。オプション D (ドリフト防止) は無関係です。オプション B はセキュリティではなくパフォーマンスに関連しています。主な目的は、悪用が発生する前にセキュリティの弱点を早期に特定することです。
参考文献：
AAIAドメイン2：AIに特有の脅威と脆弱性。
AAIAドメイン1：リスク評価と管理計画。

質問: **21**
組織のAIシステム向けデータガバナンスプログラムにおいて、成熟した効果的なアプローチを示す最適な指標は、以下のどの指標でしょうか？
A. 組織のデータセットに対するデータ品質監査の頻度

B. データ系統が文書化されているAIモデルの割合
C. 前会計年度中に完了したAIプロジェクトの数
D. 全部門におけるAI関連事業に割り当てられた総予算
正解: **B** (コメントを発表する)

質問: **22**
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、効果はあるものの、包括的で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: **23**
知的財産権およびデータ権の遵守状況を判断するために、AIシステム監査においてIS監査人が確認すべき最も重要な項目は次のうちどれですか？
A. データパフォーマンス指標
B. データ利用契約
C. オープンソースの知的財産の使用
D. モデル実行効率ログ
正解: (正解を表示します)

知的財産権（IP）およびデータ権利の遵守状況を評価するため、IS監査担当者は、所有権、ライセンス、同意、および使用制限を明記した文書化されたデータ使用契約を精査する必要があります。AAIA™学習ガイドでは、AIモデルのトレーニングまたはフィードに使用されるデータが、法的および契約上の範囲内で取得および使用されていることを確認することの重要性を強調しています。

監査担当者は、組織がデータ入力を使用、配布、または変換する適切な権利を有しているかどうかを検証するために、データ使用契約を精査する必要があります。特に、第三者データや機密データが関係する場合はなおさらです。」オープンソースの使用（C）は懸念事項ではありますが、法的明確性を提供するのはBのみです。指標（A）とログ（D）はパフォーマンスを反映するものであり、法的コンプライアンスを反映するものではありません。

参考資料：ISACA Advanced in AI Audit™ (AAIA™) 学習ガイド、セクション：「AIにおける倫理的および法的考慮事項」、サブセクション：「データ権利、ライセンス、および知的財産」

質問: **24**

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. 実際の結果を予測する際のAIモデルの精度

C. AIモデルの再学習頻度

D. AIモデルとインタラクションしているユーザー数

正解: **B** (コメントを発表する)

質問: **25**

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: (正解を表示します)

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、モデルが整列した時間ステップと一貫性のある特徴構造を受け取ることが保証され、偽のパターン、信号の欠落、および偏った予測のリスクが低減されます。

これは、AAIAがAI運用において重視するデータ品質、データバランス、およびデータ準備の方針と一致しています。

オプションBは周波数とフォーマットの違いを無視するため、ノイズや位置ずれが生じる可能性があります。オプションCは場合によっては有効ですが、複雑さとメンテナンスの負担が増大し、一貫した前処理パイプラインが必要になる場合もあります。オプションDは1つのデータソースのみを対象としており、異種センサーデータの問題を解決しません。最も堅牢な運用アプローチは、明確なデータ入力要件を定義し、トレーニング前にセンサーデータを標準化することです（オプションA）。
参考文献：
ISACA、AAIA試験内容概要 - ドメイン2：AI運用（AIに特化したデータ管理 - データ品質、データバランス、データセキュリティ）。
ISACAによる、AIモデルのためのデータパイプラインと前処理に関するAI運用ガイドライン。

質問: **26**
投資機関のAI搭載ソフトウェアの監査中に、情報システム監査担当者が潜在的なセキュリティリスクを特定しました。組織のデータを生成型AIツールに持ち出すことに関連する最大のリスクは何ですか？
A. 偏ったAIモデル出力によるデータ汚染
B. 不正なデータ開示
C. 事業の中断の可能性
D. AIが生成した知見への過度の依存
正解: **(**正解を表示します**)**
AAIA™学習ガイドでは、機密データや専有データを第三者の生成型AIツールに入力すると、不正なデータ漏洩につながる可能性があることを強調しています。これらのツールは入力データを保存、処理、または再学習する可能性があり、プライバシーや知的財産権のリスクが生じる可能性があります。
「従業員が機密データを外部のAIツールに入力すると、組織はその情報に対する制御を失うリスクを負います。これは、規制違反、法的責任、および取り返しのつかないデータ漏洩につながる可能性があります。」事業の中断（C）と依存（D）は注目に値しますが、最も深刻で差し迫ったリスクはBの不正開示です。データ汚染（A）は、データのセキュリティではなく、モデルの信頼性に影響を与えます。
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：「データプライバシーと外部AIツールの使用」

質問: **27**
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. 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。

B. データ属性「product flavor」のオプション（バニラ、チョコレート、ストロベリー、バナナ）のダミー変数を作成します。
C. データ属性「犬種」のオプション「ラブラドール」「チワワ」「ビーグル」に対応するダミー変数を作成します。
D. 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する。
正解: **(**正解を表示します**)**

質問: **28**
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. 適時性
B. 予測可能性
C. 代表性
D. 理解しやすさ
正解: **C (**コメントを発表する**)**
代表性を確保することで、トレーニングデータがAIモデルが実運用環境で遭遇するあらゆる状況を網羅的に反映することが保証されます。AAIA™学習ガイドによると、代表性のないデータでトレーニングされたモデルは、バイアスが生じやすく、汎化性能が低く、実世界のアプリケーションで性能が低下する傾向があります。
「トレーニングデータが運用環境を正確に反映していることを保証することは、モデルの信頼性、公平性、拡張性にとって極めて重要です。それがなければ、モデルはテストでは良好な結果を示しても、実際の使用では失敗する可能性があります。」適時性（A）と理解しやすさ（D）はパフォーマンスとユーザビリティを支えますが、データカバレッジの確保に比べれば二次的なものです。予測可能性（B）は、動的モデリングにおいては必ずしも望ましいとは限りません。
参考資料：ISACA Advanced in AI Audit™ (AAIA™) 学習ガイド、セクション：「AIの基礎と技術」、サブセクション：「トレーニングデータの特性とモデルの妥当性」

質問: **29**
医療機関が患者データを用いて、早期疾患検出のためのAIモデルを訓練している。個人データの安全性と完全性を確保する上で、次のうちどれが最も確実な方法だろうか？
A. 保存データを暗号化して情報漏洩とログアクセスを削減
B. 新しいデータと追跡変更を用いてAIモデルを更新する
C. 厳格なデータアクセス制御の実施とセキュリティテストの実施
D. 患者データの匿名化と定期的な品質チェックの実施
正解: **D (**コメントを発表する**)**
医療AIアプリケーションにおいて、患者データの保護は極めて重要です。AAIA™学習ガイドでは、プライバシーを保護し、データの完全性を維持するための最も効果的な戦略の一

つとして匿名化を挙げています。匿名化を品質チェックと組み合わせることで、データの正確性と医療データ保護規制（HIPAA、GDPRなど）への準拠が保証されます。
機密データを匿名化することで識別情報が削除され、データへのアクセスや漏洩のリスクが大幅に軽減されます。継続的なデータ品質チェックにより、匿名化されたデータセットの完全性と有用性が保証されます。」暗号化（A）とアクセス制御（C）は必要な技術的保護策ですが、Dはプライバシーと正確性の両方を最も強力に保証します。オプションBは、データセキュリティよりもモデル管理に重点を置いています。
参考資料：ISACA Advanced in AI Audit™ (AAIA™) 学習ガイド、セクション：「AIにおける倫理的および法的考慮事項」、サブセクション：「機密性の高いAIデータのプライバシーとセキュリティ」

質問: **30**
ある組織が、顧客チャットログを使用して学習させたAI搭載の顧客サービスチャットボットを導入しました。リスク評価において、IS監査担当者が最も懸念すべき問題はどれでしょうか？
A. AIモデルが新しいデータを取り込む能力が限られている
B. 旧式の手順により、データ整合性の検証が不十分になっている。
C. チャットボットの不正確な応答による評判への影響
D. アクセス制御の不備により、顧客データが不正に漏洩する。
正解: **(**正解を表示します**)**
最大の懸念事項は、アクセス制御の不備（D）であり、これは顧客データの不正な漏洩につながり、プライバシー、セキュリティ、規制、および評判に重大なリスクをもたらします。チャットログには、個人を特定できる情報や機密性の高い通信が含まれていることがよくあります。AAIAは、特に顧客と対話するAIシステムにおいて、データの機密性、アクセス制御、およびプライバシー義務を最もリスクの高い要素として優先的に取り上げています。チャットボットの応答が不正確であること（C）は評判に影響しますが、データ漏洩ほど深刻ではありません。手順が古くなっていること（B）は問題ですが、差し迫った被害は少ないです。データを取り込む能力が限られていること（A）はパフォーマンスに影響しますが、重大なリスクではありません。
参考文献：
ISACA、AAIA試験内容概要 - ドメイン5：法的およびプライバシーに関する考慮事項、ドメイン1：AIガバナンスとセキュリティ管理。

質問: **31**
ある小売企業は、顧客の購入履歴を分析してパーソナライズされた割引を提供するために、AIモデルを使用しています。以下のどの方法が、顧客データの最も倫理的な利用方法と言えるでしょうか？
A. 顧客の購入データは、明示的な同意を得た後にのみ利用し、顧客がオプトアウトできるようにする。

B. 収集した顧客情報のデータセットを一般の人々が閲覧・監査できるようにする。
C. 広告およびコミュニケーションの改善のため、顧客の購入データを第三者ベンダーと共有する。
D. 偏りのない推奨事項を保証するために、利用可能なすべての顧客データを保持および分析します。
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　275問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **32**
AIシステムの監査を行う際、AIモデルの動作が組織の目標と一致していることを確実にするには、次のうちどの手順が適切でしょうか？
A. アルゴリズムのデバッグ
B. データ変換
C. モデルトレーニング
D. 問題設定
正解: (正解を表示します)
問題設定（オプションD）とは、AIシステムを構築または展開する前に、その目的、範囲、および望ましい成果を明確に定義するプロセスです。ISACA AAIA™学習ガイドによると、「問題設定は、モデル開発とその後の動作を組織の戦略的および運用上の目標に整合させるための重要な第一歩です。」AIの問題が組織の目標に沿って設定されていない場合、技術的に優れたAIモデルであっても、組織の使命や優先事項をサポートしない出力を生成する可能性があります。
アルゴリズムのデバッグ、データ変換、モデルのトレーニングはすべて重要な段階ですが、それらの取り組みが正しく方向付けられるためには、最初の問題設定が不可欠です。
参考資料：「ISACA Advanced in AI Audit™ (AAIA™) 学習ガイド、セクション：「AIプロジェクトライフサイクルアライメント」

質問: **33**
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. 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。
B. 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。

C. 信頼できるデータセットが利用可能であることを保証する。
D. 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。
正解: **(**正解を表示します**)**
AAIA™学習ガイドでは、高性能かつ倫理的なAIシステムの基盤は、データの質と完全性にあることを強調しています。医療、金融、刑事司法などで使用されるような高リスクのAIシステムにおいては、信頼できるデータに基づいてモデルを構築することが不可欠です。これにより、信頼性の高い予測が保証され、バイアスが軽減され、リスクが緩和されます。
「信頼できるデータセットは、正確性、完全性、一貫性、倫理的な情報源によって特徴づけられます。リスクの高いAIアプリケーションでは、あらゆる段階でデータ品質を確保することが、システムの信頼性とコンプライアンスにとって極めて重要です。」バックアップ、ユーザー研修、多要素認証はセキュリティと運用上の回復力にとって重要ですが、開発および設計段階でモデルの正確性と公平性を確保するという根本的な課題には対処していません。
したがって、選択肢Cが最も効果的な方法である。
参考資料：ISACA Advanced in AI Audit™ (AAIA™) 学習ガイド、セクション：「AIの基礎と技術」、サブセクション：「データガバナンスと管理」

質問: **34**
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: **C (**コメントを発表する**)**
著しく高い拒否率は、アルゴリズムによる差別の可能性を示す明確な指標です。経営陣は、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）を実施することを第一の対応策とすべきです。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ます。
選択肢Aは、公平性の問題がほとんどのリスク許容範囲を超えるため、受け入れられません。選択肢Bは手続き上のチェックであり、解決策ではありません。選択肢D（データの統合）は役立つかもしれませんが、根本原因が特定された後でなければならず、最初の重要なステップではありません。
参考文献：
ISACA、AAIA試験内容概要 - ドメイン1：偏見、公平性、透明性の評価。

質問: **35**

ある医療機関が胸部X線画像を分析するAIモデルを導入しました。このモデルは高い精度を報告していますが、その閾値は不明確であり、患者の属性別の性能分析も行われていません。なぜ精度だけではこのモデルを評価するには不十分なのでしょうか？
A. このモデルは特定のグループに対して性能が低下する可能性があり、隠れた公平性リスクにつながる可能性があります。
B. 精度は構造化された表形式のデータセットでのみ計算できます。
C. 高い精度スコアは常に低い偽陽性を示します。
D. パフォーマンスはすべての人口統計学的サブグループで同一です。
正解: **(**正解を表示します**)**
ISACA AAIA™マニュアルは、医療などの高リスクな用途における 集計精度」について警告している。
あるモデルは全体としては95%の精度であっても、特定の少数派グループ（例えば、年齢や民族に基づく）では40%のエラー率を示す場合があります。これは、特定のグループの患者が一貫して誤診されるという 隠れた公平性と安全性のリスク」を生み出します。監査担当者は、公平な結果と患者の安全性を確保するために、各サブグループごとにパフォーマンス指標（精度 再現率）を個別に計算する 層別評価」を推奨する必要があります。

質問: **36**
以下の前処理手順のうち、非技術系の関係者に対してAIモデルの決定を最も効果的に正当化できるのはどれでしょうか？
A. 順列特徴量の重要度
B. ローカルで解釈可能なモデル非依存の説明（LIME）
C. 部分依存プロット
D. AIモデルの侵入テスト
正解: **(**正解を表示します**)**
記載されているすべての手法（侵入テストを除く）は解釈可能性をサポートしていますが、ISACA AAIA™ 学習ガイドでは、個々の意思決定を説明できる点において LIME」が特に注目されています。LIMEは、特定の予測に基づいて、どの特徴（例えば、高収入や低負債）がその特定のケースの主な要因であったかを示す、よりシンプルで解釈しやすいモデルを作成します。この ローカル」な説明は、モデル全体の動作を説明する特徴重要度（オプションA）や部分依存プロット（オプションC）といった グローバル」な指標よりも、技術的な知識を持たない関係者や顧客にとって理解しやすいものです。

質問: **37**
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. 訓練データ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: **38**
AIを活用した監査ツールの最も重要な属性は次のうちどれですか？
A. モデル結論の説明可能性
B. 監査リソースの最適化
C. ラベル付きトレーニングデータセットの使用
D. 多様な統計手法に対応
正解: **(**正解を表示します**)**
ISACA AAIA™学習ガイドによると、透明性はAI監査の要です。監査人がAI駆動ツールに依拠するためには、そのツールが「説明可能性」、つまり特定の結論や異常がどのように特定されたかを説明できる能力を備えている必要があります。説明可能性がなければ、AIは「ブラックボックス」のままであり、監査人が職業的懐疑心を発揮したり、利害関係者に対して監査結果を正当化したりすることができなくなります。リソースの最適化や統計情報の裏付けは有益ですが、モデルのロジックが健全で偏りがなく、規制基準に準拠しているという必要な保証を提供するものではありません。監査人は、説明責任を確保するために、自動化された決定の根拠を検証する必要があります。

質問: **39**
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: **(**正解を表示します**)**

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: **40**

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. ローカル解釈可能モデル非依存説明（LIME）を使用して、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。AAIA™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し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。」オプションA、B、Cは技術的なモデリング手法ですが、利害関係者にとって分かりやすい説明を優先していません。

したがって、透明性という点ではDが最適である。

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：「説明可能性ツールとステークホルダーとのコミュニケーション」

質問: **41**
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: **(**正解を表示します**)**
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、モデルがトレーニング中に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します。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分割されていることを確認する必要があります。」オプションA、C、Dは処理順序または量に関するものですが、重複データによるモデル整合性の損なわれという根本的な問題に対処しているのはB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の基礎と技術」、サブセクション：「データ分割と漏洩リスク」

質問: **42**
データ異常を分析するために予測型AIツールを使用する際、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. AIツールによって生成された偽陽性または偽陰性
B. AIツールを既存のデータ監査ソフトウェアに容易に統合できること
C. AIツールが大規模データセットを処理する速度
D. データ監査目的でAIツールを導入・維持するための費用
正解: **A (**コメントを発表する**)**
異常を分析する予測型AIツールにとって、最大の懸念事項は、偽陽性と偽陰性の発生率と影響です(A)。偽陽性は不必要な調査につながる可能性があり、偽陰性は真の問題(不正、統制の不備など)が見過ごされることを意味します。保証の観点から見ると、偽陰性は監査目標を直接的に損なうため、特に重要です。AAIAは、監査で使用されるAIツールを評価する際には、主要なパフォーマンス指標(精度、再現率など)とエラーのトレードオフが不可欠であることを強調しています。
統合の容易さ（B）、速度（C）、コスト（D）は重要な実務上の考慮事項ですが、ツールが重大な異常を正確に特定できるか、あるいは見逃してしまうかという点に比べれば二次的なもの

です。したがって、誤検出（偽陽性および偽陰性）といったエラー挙動こそが、監査品質に対する主要なリスクとなります。
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、ドメイン2：AI運用（モデルのパフォーマンス指標とリスク）。
ISACAによる、監査の文脈における精度、再現率、およびエラー分析を用いたAIツールの評価に関する分析ガイダンス。

質問: **43**
IS監査担当者が、複数のデータソースを含む証拠収集のためのAIツールの導入状況を評価しています。AIを活用した証拠収集によって監査プロセスが改善されたことを最もよく示す結果は、次のうちどれでしょうか？
A. AIモデルの再学習を可能にする、報告期限の延長
B. データ収集にかかる時間を短縮し、証拠収集におけるエラーを減らす。
C. データおよび証拠分析における人間の判断の排除
D. 最小限のデータクレンジングで非構造化データに依存できる能力
正解: **(正解を表示します)**
AIを活用した証拠収集は、効率性と正確性を向上させるはずです。改善の最も優れた指標は、データ収集にかかる時間の短縮とエラーの減少（B）であり、AIが品質を損なうことなく、データの抽出、統合、および初期検証を効率化していることを示しています。AAIAの監査プロセスにおけるAIに関するコンテンツでは、反復作業の自動化、カバレッジの向上、より質の高い証拠といったメリットが強調されています。
再訓練に長期間を要すること（A）は、改善というよりむしろ非効率性を示唆している。人間の判断を排除すること（C）は現実的でも推奨されることでもなく、専門家の懐疑心と監査人の判断は依然として不可欠である。最小限のデータクレンジングしか行わない非構造化データに依存すること（D）は、誤解釈やノイズのリスクを高める可能性がある。したがって、より効率的かつ正確な証拠収集こそが、最も明確なプラスの成果である。
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（監査における効率と品質の向上）。
ISACAによる内部監査およびデータ分析に関するガイダンス：証拠収集におけるAIの価値について。

質問: **44**
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. 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

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. 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。
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: **(**正解を表示します**)**

質問: **45**
IS監査担当者は、監査サンプリングプロセスにAI技術を統合することを検討しています。以下のうち、監査担当者が大規模なデータセットの中から高リスクの取引を特定し、対象を絞ったサンプリングを行うために最も有効な方法はどれですか？
A. 自然言語処理（NLP）
B. 光学文字認識（OCR）
C. ルールベース分析
D. 予測分析
正解: **D (**コメントを発表する**)**
予測分析は、統計モデル、異常検知、機械学習を用いて高リスク取引を特定する最も効果的な方法です。
* 固有リスクと残存リスクに基づいて取引をランク付けする
監査担当者が手動では特定できない隠れたパターンを検出する
* 異常な取引プロファイル、外れ値、および危険信号を強調表示します
* より詳細な調査が必要な取引を優先する
AAIAの監査分野では、AIによって強化されたリスクベースのサンプリングが重視されており、予測モデルによって網羅性と精度が大幅に向上する。
NLP（A）はテキストから洞察を抽出するが、取引リスクスコアリングには最適ではない。
OCR（B）は文書をデジタル化するが、リスクを特定する機能はない。
ルールベース分析（C）は既知のパターンしか捉えませんが、予測分析は未知のリスクや新たなリスクを明らかにします。
参考文献：
AAIAドメイン3：監査プロセスにおけるAI（高度な分析、異常検知、リスクスコアリング）。

質問: **46**
IS監査担当者が、大学が予測機械学習モデルのトレーニングに使用したデータセットをレビューしています。モデルがすべてのデータを処理して必要な相関関係を導き出せないリスクを最も示唆しているのは、次のうちどれでしょうか？
A. 学生番号フィールド（整数形式）
B. 学年レベルフィールド（float形式）
C. オブジェクト形式の最終成績パーセントフィールド
D. ブール形式の学士号を取得していること
正解: **(**正解を表示します**)**

オブジェクト（文字列）形式（オプションC）で保存された数値フィールドは、データ型が不適切であることを示しています。数値がテキストデータとして保存されている場合、モデルは相関関係や統計的関係を正しく計算できません。
AAIAは、不適切なデータ型が機械学習モデルの誤動作の最も一般的な原因の1つであることを強調しており、その例として以下が挙げられます。
平均値、相関関係、または数学的演算の計算に失敗した
* 前処理におけるサイレントエラー
学習パターンの偏り
* 機能の重要度評価が不正確であるため、オブジェクト形式の最終成績パーセントフィールドが処理リスクの最も重要な指標となります。オプション A、B、および D は、それぞれのフィールドに対して有効なデータ型であり、モデル処理に固有のリスクはありません。
参考文献：
AAIA ドメイン2：データ品質、データ型、および前処理。
AAIA ドメイン3：AI対応状況とデータ検証。

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　**275**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **47**
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. データの層別化
B. データのクリーニング
C. システムのトレーニング
D. システムの隔離
正解: **(**正解を表示します**)**

質問: **48**
IS監査担当者は、AIモデルがテストデータよりもトレーニングデータで著しく優れた結果を達成したことに気づきました。IS監査担当者は、このモデルに関して以下のどの問題点を特定したのでしょうか？
A. アンダーフィッティング
B. 過学習
C. バイアス
D. 一般化

正解: **B** (コメントを発表する)

質問: **49**
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: (正解を表示します)
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。AAIA™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が困難な異常、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。
参考資料：ISACA Advanced in AI Audit™ (AAIA™) 学習ガイド、セクション：「AIを活用した監査アプローチの利点」

質問: **50**
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: **51**
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. 定期的な卓上運動の実施
B. 主要リスク指標（KRI）を定期的に更新する
C. 混乱発生時のキルチェーンプロセスの実施
D. 災害復旧計画（DRP）に、AIによる障害発生時の様々なシナリオを含める
正解: **D** (コメントを発表する)

質問: **52**
金融機関の顧客サービスチャットボットが、ユーザーに誤った法的助言を提供することがあり、その結果、顧客からの苦情が多数発生し、規制当局から問題視される可能性もある。このリスクを軽減するために、まず最初に行うべきことはどれか？
A. チャットボットのトレーニングデータセットを拡張します。
B. より多様なデータセットでチャットボットを再学習させる。
C. 人間が関与するレビュープロセスを導入する。
D. チャットボットの技術文書を確認する。
正解: (正解を表示します)
顧客対応システムが有害または誤ったアドバイス（特に法律または財務に関するもの）を提供している場合、「最優先事項」は、さらなる被害を防ぐことです。「人間が関与するレビュープロセスを導入する」ことで、資格のある人間がチャットボットのアドバイスを顧客に送信する前に確認し承認することが保証されます。これは、即時の安全「ガードレール」として機能します。再トレーニング（オプションAおよびB）は、時間がかかる長期的な解決策であり、現在の誤った出力を止めることはできません。ISACAによると、人間の監視は、リアルタイムの顧客とのやり取りにおける重大なエラーを軽減するための最も効果的な事後制御です。

質問: **53**
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: **54**
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。AAIA™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。
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システムにおけるデータプライバシーと情報保護」

質問: **55**
新しいAIソリューションのデータガバナンス計画を作成するのに最適な時期は、次のうちどれでしょうか？
A. テスト段階中
B. 生産開始前
C. 初期設計の一部として
D. データ収集中

正解: (正解を表示します)
AI開発において、「プライバシー・バイ・デザイン」と「ガバナンス・バイ・デザイン」は基本原則です。データガバナンス計画は、「初期設計段階」で策定されるべきです。これにより、データ品質、データリネージ、ラベリング、プライバシーに関する要件が、最初からアーキテクチャに組み込まれることが保証されます。
AAIA™フレームワークによれば、テスト段階（オプションA）または本番環境段階（オプションB）でガバナンスを後付けしようとすると、データが既に破損していたり、コンプライアンスに準拠していない方法で収集されている可能性があるため、多くの場合、不可能または費用がかかりすぎる。設計段階で計画を立てることで、欠陥のある基盤の上に構築してしまうリスクを軽減できる。

質問: **56**
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。AAIA™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、匿名化も重要ですが、入力データの関連性と適合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。
参考資料：ISACA Advanced in AI Audit™ (AAIA™) 学習ガイド、セクション：「生成型AIのための入力データガバナンス」

質問: **57**
IS監査担当者が、社内で開発された生成型AIツールを使用して、監査関係者向けの状況報告を作成します。監査担当者にとって最も適切な行動は次のうちどれですか？
A. 提供された情報が完全かつ正確であるかどうかを評価します。
B. 結果を再生成して、同様の出力が得られるようにします。
C. 結果を公開されている生成AIツールと比較し、出力が類似していることを確認します。
D. 結果を経営陣と共有し、検討する。
正解: (正解を表示します)

質問: **58**
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. 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リスク評価
B. 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
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. 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
正解: **C** (コメントを発表する)

質問: **59**
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、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: **60**
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 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は価値の高いエントリを優先します。
正解: (正解を表示します)

質問: **61**
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由来
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。

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　**275**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **62**
モデルのアーキテクチャ、重み、ハイパーパラメータを保護するために最も効果的な制御方法は次のうちどれですか？
A. AI技術セキュリティのベストプラクティスに関する従業員向け研修を実施する。
B. モデルにアクセスする前に、ユーザーに機密保持契約への署名を求める
C. トレーニングデータの逸脱に関する詳細なデータ監査ログを保持する
D. モデルコンポーネントに対して厳格なアクセス制御と暗号化を実装する
正解: **(**正解を表示します**)**
独自のAIモデルコンポーネント（アーキテクチャ、重み、ハイパーパラメータ）を保護する最も効果的な方法は、厳格なアクセス制御と暗号化（オプションD）です。

AAIAは、モデルの盗難とリバースエンジニアリングを重大なセキュリティリスクと位置付けており、特にAIモデルに組み込まれた知的財産によって競争優位性を得ている組織にとっては深刻なリスクとなる。
適切な管理策には以下が含まれます。
* 役割ベースアクセス制御（RBAC）
* 保存時および転送時の暗号化
* モデルレベルのアクセス分離
* ハードウェアセキュリティモジュール（HSM）
* ゼロトラストアクセス原則
訓練（A）は意識を高めるが、保護を強制するものではない。
機密保持契約（B）は法的拘束力を持つが、技術的な侵入を防ぐものではない。
監査ログ（C）はトレーニングデータを追跡しますが、モデル自体を保護するものではありません。
したがって、暗号化とアクセス制御が最も強力な保護手段となる。
参考文献：
AAIAドメイン2：AIセキュリティと知的財産保護
AAIAドメイン1：アクセス制御とセキュリティ対策

質問: **63**
IS監査担当者は、社内で開発された生成型AIツールを使用して、監査関係者向けの状況報告を作成する。
監査人が取るべき最も適切な行動はどれですか？
A. 結果を公開されている生成AIツールと比較し、出力が類似していることを確認します。
B. 提供された情報が完全かつ正確であるかどうかを評価します。
C. 結果を再生成して、同様の出力が得られるようにします。
D. 結果を経営陣と共有し、検討する。
正解: **B (**コメントを発表する**)**
AIツールを使用してレポートや更新情報を生成する監査担当者は、出力が信頼性が高く、事実に基づき正確で、完全であることを確認しなければなりません。AAIA™学習ガイドによれば、生成型AIがコンテンツ作成を支援する場合でも、監査コンテンツに対する責任は監査担当者にあります。したがって、AIが生成したコンテンツの完全性と正確性を検証することが、監査担当者の第一の責任となります。
「AIが生成した監査出力は、ソースデータおよび専門基準に照らして検証されなければならない。監査人はAIの貢献を批判的に評価し、人間の監視なしにそれらに依存してはならない。」オプションAとCは出力の一貫性に焦点を当てており、正確性には焦点を当てていない。オプションDは検証ではなく、コミュニケーション段階の一部である。したがって、Bが監査人の主要な責務である。
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：「AI支援タスクにおける監査人の責任と検証」

質問: **64**
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: **B (**コメントを発表する**)**
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: **65**
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を使用して監査レポートを作成する際の最大のリスクは、統制の有効性を誤って表現する可能性があることです B)。
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ことによって、監査全体の信頼性が損なわれ、不適切な経営判断、規制上の問題、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: **66**
IS監査担当者は、ウォークスルー会議から得られた監査報告書を作成するために、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ており、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: **67**
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ます（赤、青、緑、黒、白）。
B. 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。
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. オプションの製品フレーバーのデータ属性（バニラ、チョコレート、ストロベリー、バナナ）のダミー変数を作成します。
正解: **(**正解を表示します**)**
AAIA™学習ガイドでは、カテゴリ変数をエンコードする際には、関連するカテゴリの意味と順序を維持する必要があることを強調しています。最も大きなリスクは、顧客報酬ティアなどの順序データがワンホットエンコーディングによって名義データとして扱われる場合に発生します。ワンホットエンコーディングでは本来の順序が失われ、モデルの学習に悪影響を与える可能性があります。
順序変数を名義変数として不適切にエンコードすると、モデルが関係性を正しく理解できなくなり、予測精度が低下したり、結果に偏りが生じたりする可能性があります。」顧客報

酬カテゴリ（エコノミー＜ビジネス＜ファーストクラス）には自然な順序があります。ワンホットエンコーディングはこの順序を無視するため、モデルの精度が低下する可能性があります。その他のオプションは名義データを表し、適切にエンコードされています。
参考資料：ISACA Advanced in AI Audit™ (AAIA™) 学習ガイド、セクション：「AIの基礎と技術」、サブセクション：「データ前処理と特徴量エンジニアリング」

質問: **68**
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提出する
B. 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
C. 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
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: **(**正解を表示します**)**

質問: **69**
ラベル付けされていないデータ要素内の制御効果における根本的なパターンを最も適切に特定するために使用できるのは、次のうちどれですか？
A. XGBoost学習
B. 強化学習（RL）
C. 教師なし学習
D. ランダムフォレスト
正解: **(**正解を表示します**)**
データが「ラベルなし」（つまり、結果や「回答」が提供されていない）の場合、ランダムフォレスト（オプションD）やXGBoost（オプションA）などの教師あり学習手法は使用できません。「教師なし学習」は、人間の介入なしにデータ内の「潜在的なパターン」、クラスター、または潜在構造を発見するために特別に設計されています。監査担当者にとって、教師なし学習手法（クラスタリングなど）は、類似の統制上の失敗をグループ化したり、不正または正当なものとしてまだ分類されていない異常な取引行動を特定したりするなど、探索的分析に非常に役立ちます。

質問: **70**
プライバシー規制に基づくユーザーデータ所有権をAIシステムが確実に遵守するために、最も適切な方法はどれですか？
A. データクラスタリング技術を適用してデータセットを匿名化する
B. 厳格なデータ保持ポリシーを適用し、保存期間を制限する
C. 透明性の高いデータ同意管理プロセスの導入
D. AIシステムの精度を検証するための性能テストを定期的に実施する
正解: **(**正解を表示します**)**

透明性の高いデータ同意管理プロセスは、ユーザーが自身のデータがどのように使用されるかを把握し、同意、アクセス、訂正、削除といった権利を行使できるようにするものです。これは、GDPRやCCPAなどの規制における重要な要件です。
同意管理は、データ所有権を尊重する上で不可欠です。組織は、データの使用目的を明確に開示し、オプトイン/オプトアウト機能を提供し、ユーザー操作の監査証跡を維持する必要があります。」匿名化および保持ポリシーはコンプライアンスをサポートしますが、ユーザーの制御には対応していません。パフォーマンス テスト（D）はモデルの精度に関係するもので、ユーザーの権利とは関係ありません。したがって、C が最適な答えです。
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：「ユーザーデータ権利と同意管理」

質問: **71**
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. 予測アルゴリズムの単体テスト
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. 入力変数に関する感度分析
正解: **(**正解を表示します**)**

質問: **72**
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: **B (**コメントを発表する**)**
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、AAIA™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。
公平性を評価するには、監査人は管理されたデータセットを使用して、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るかどうかを評価する必要があります。この実証的なテストは、定性的な方法よりも強力な証拠を提供します。」メタデータ（A）と開発者へのインタビュー（C）は調査結果を補完できますが、客観的で再現可能な証拠を提供するの

はBのみです。オプションDは現実世界の相互作用を反映している可能性がありますが、監査に必要な管理と一貫性が欠けています。
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システムにおける公平性とバイアスのテスト」

質問: **73**
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。
B. 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。
C. 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。
D. 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。
正解: **C** (コメントを発表する)

質問: **74**
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。AAIA™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、偏ったトレーニング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。」コスト（A）と業界の成熟度（B）は考慮事項ではありますが、これらは同じ体系的な倫理的リスクをもたらすものではありません。
抵抗（D）は変革管理上の課題である。Cは最も影響力が大きく、広範囲に及ぶリスクを表す。
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：AIにおけるバイアスと公平性」

質問: **75**
ある組織が、社内業務処理に市販の生成型AIソリューションを利用している。責任共有の原則に基づくと、以下のどの領域が組織の主要な責任範囲となるか？
A. 基盤となるAIコンピューティングインフラストラクチャの維持
B. 基礎モデルの初期トレーニングを実施する
C. モデルの中核となる安全・セキュリティシステムが堅牢に設計されていることを保証する
D. 適切な利用ポリシーを定義し、IDおよびアクセス管理（IAM）を実施する
正解: **(**正解を表示します**)**
「サービスとしてのソフトウェア」（SaaS）または既製のAIモデルの導入においては、「責任共有モデル」に基づき、ベンダーは「モデルのセキュリティ」（インフラストラクチャ、基本トレーニング、コアセキュリティ）に責任を負い、顧客は「モデル内のセキュリティ」（使用方法）に責任を負います。組織の主な責務は、「使用ポリシーを定義し、IAM（アイデンティティおよびアクセス管理）を徹底すること」であり、承認された従業員のみがツールを使用し、機密性の高い企業データを未検証のプロンプトに入力しないようにすることです。このガバナンスにより、AIが組織固有の運用環境において倫理的かつ安全に使用されることが保証されます。

質問: **76**
以下のAIのうち、ラベル付けされていないデータセットを使用して人間の学習行動を模倣できるのはどれですか？
A. 教師あり学習
B. 連合学習
C. 強化学習
D. 教師なし学習
正解: **D (**コメントを発表する**)**
教師なし学習は、ラベル付けされていないデータを使用して、明示的な結果ラベルなしにパターン、構造、またはグループを発見します。モデルは、データ内の類似点、クラスター、または潜在的な構造を識別することによって「学習」します。これは、人間が正解を教えられなくてもパターンに気づく方法とある程度似ています。AAIAの基礎解説では、教師なし手法（クラスタリング、次元削減など）は、ラベルが利用できない、またはラベル付けにコストがかかるものの、洞察が必要な状況に明確に関連付けられています。
教師あり学習（A）は、ラベル付きの例（入力と出力のペア）を必要とします。連合学習（B）は、ラベル付けの要件そのものではなく、分散型トレーニングのパラダイムを説明するものです。強化学習（C）は、ラベルなしの静的データセットではなく、報酬と罰則の形でフィードバックを利用します。したがって、ラベルなしデータを直接使用して構造を学習する正しいタイプは、教師なし学習です。
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（教師あり学習、教師なし学習、強化学習）。
ISACAのAI基礎講座における、学習の種類とデータラベリングに関する内容。

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　**275**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **77**
ある組織の採用選考プロセスで使用されているAIモデルが、特定の性別の候補者を優遇していることが判明した。このAIモデルは、新規採用者の大多数が男性である採用記録に基づいて学習されていたことが指摘されている。これはどのようなバイアスを最もよく示しているだろうか？
A. ラベル
B. 地理
C. 確認
D. 歴史的
正解: **(**正解を表示します**)**
歴史的バイアス」とは、トレーニングデータが既存の社会的偏見や過去の不平等を反映している場合に発生します。組織の過去の採用慣行が男性を優遇していた場合、その記録に基づいてトレーニングされたAIモデルは、男性であることが採用される候補者の特徴であると「学習」します。これは、過去の差別を自動化し、将来の意思決定に永続させることになります。AAIA™マニュアルでは、監査人は公平性を確保するために、トレーニングデータにおける歴史的バイアスを評価する必要があると強調しています。確証バイアス（既存の信念を裏付けるデータを探すこと）やラベルバイアス（誤った分類を行うこと）とは異なり、歴史的バイアスは、欠陥のある現実世界の環境からデータを収集することに起因する体系的な問題です。

質問: **78**
データ処理における機械学習（ML）の主な目的は以下のとおりです。
A. データセットを分析して、視覚的なパターンと傾向を特定します。
B. AIモデルの出力の説明可能性を高める。
C. 通常、人間の知能を必要とする行動を実行する。
D. 人工人間知能を作成するための統計的推論を行う。
正解: **C (**コメントを発表する**)**

AAIA™学習ガイドでは、機械学習の核心的な目的を、システムがデータから学習し、通常は人間の認知機能を必要とする意思決定やタスクを実行できるようにする能力と定義しています。機械学習により、AIシステムはパターンを識別し、過去のデータから学習し、複雑な意思決定を自動化することができます。

「機械学習は、パターン認識、言語理解、意思決定など、人間の知能の側面をシミュレートするシステムを育成します。これは、人間の作業を代替または補完するように設計された多くのAIアプリケーションの基盤となっています。」視覚分析（A）と統計的推論（D）は機械学習の機能ですが、これらはサブセットであり、主要な目標ではありません。説明可能性（B）は重要ですが、機械学習の中核機能ではありません。したがって、Cが主要な目的を最もよく表しています。

参考資料：ISACA Advanced in AI Audit™ (AAIA™) 学習ガイド、セクション：「AIの基礎と技術」、サブセクション：「機械学習の基礎と目的」

質問: **79**

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に基づく信用スコアリングでは、モデルの複雑さゆえに、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。入力の検証と異常検出が不十分な場合、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ります。ISACA AAIA™フレームワークによれば、これらの偏った入力によって、モデルは大規模データセットに隠された差別的なパターン（例えば、民族性と信用度との相関関係）を学習してしまう可能性があります。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ります。過学習（オプションB）とコスト（オプションC）は技術的な懸念事項ですが、チェックされていない入力による自動差別のシステムリスクは、組織の法的地位と評判にとって最も重大な脅威となります。

質問: **80**

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: **81**
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、一貫性のある区切り文字、適切なエンコーディングなど）がなければ、AIツールは失敗したり、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: **82**

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. モデルの学習に使用するデータを強化する。
B. 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。
C. 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。
D. 例外措置について取締役会の承認を得る。
正解: **(**正解を表示します**)**

質問: **83**
組織内でAIソリューションに特化した堅牢なデータガバナンスフレームワークを導入することによる主なメリットは次のうちどれですか？
A. AIモデル予測の精度と信頼性の向上に重点を置いています。
B. データ準備プロセスを完全に自動化することで、AI導入の期間を短縮します。
C. 業界規制の遵守を促進し、データ漏洩やプライバシー侵害のリスクを最小限に抑えます。
D. 人手による監視の必要性を減らし、シームレスで自律的なデータガバナンスを実現します。
正解: **(**正解を表示します**)**
AAIA™学習ガイドによると、堅牢なデータガバナンスフレームワークは、AIシステムがデータ保護法、倫理基準、および社内ポリシーに準拠していることを保証します。また、データ品質、アクセス、保持、処理に関する管理機能を提供し、これらはすべて情報漏洩を回避し、信頼を維持するために不可欠です。
 強力なデータガバナンス構造は、規制遵守と倫理的なAI実践の基盤となります。これにより、AIライフサイクル全体を通してデータのプライバシー、完全性、および使用権が維持されます。」オプションAは優れたデータガバナンスの結果であり、自動化（B）は効率性を向上させる可能性がありますが、最も根本的な利点はリスク軽減とコンプライアンス（C）です。オプションDは、人間の監視を必要とするガバナンスに対する誤解を反映しています。
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：「データガバナンスフレームワークとコンプライアンス」

質問: **84**
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: **85**
ある組織が、明確なデータ所有権ポリシーを定めずに、複数の外部ソースからのデータを統合するAIシステムを開発しています。この状況において、最も懸念されるのは次のうちどれでしょうか？
A. AIモデルの精度を検証する方針と手順に欠陥がある
B. ユーザーアクセス権限に関するドキュメントが限定的
C. 自動データ収集とデータクレンジングへの過度の依存
D. AIプライバシーコンプライアンスと説明責任におけるギャップ
正解: **(**正解を表示します**)**
複数の外部ソースからのデータを統合する場合、データの所有権が不明確だと、プライバシー、同意、保持、および合法的な処理に関する説明責任に直接影響します。これは、AIプライバシーのコンプライアンスと説明責任（オプションD）にギャップを生み出し、違反は規制上の制裁、訴訟、および深刻な評判の失墜につながる可能性があるため、最大の懸念事項となります。AAIAのガバナンスとリスクの領域では、明確な役割、責任、および所有権を含むプライバシーとデータガバナンスプログラムを重視しています。
オプションAは重要ですが、正確性とパフォーマンスの検証に関わるものであり、根本的な法的問題や説明責任の問題とは直接関係ありません。オプションB（アクセス権限）は管理上の問題ですが、所有権と責任が明確になれば通常は容易に解決できます。オプションC（自動データ収集／データクレンジングへの依存）は品質リスクをもたらす可能性がありますが、誰が責任を負うのかを直接的に解決または定義するものではありません。したがって、主なリスクは、外部データソース全体にわたる明確なプライバシーと説明責任の構造の欠如です。
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（データガバナンス、プライバシーに関する考慮事項）。
ISACAによる、AIガバナンス、役割、責任、およびデータ利用に関する説明責任についてのガイダンス。

質問: **86**
IS監査担当者が、自律的な対応のために「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。以下のうち、最も重要な考慮事項はどれですか？
A. エージェントの動作にはネットワーク拡張が必要です。
B. このエージェントはアナリストの介入の必要性を軽減します。
C. エージェントの監査ログが長くなり、ストレージコストが増加します。
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、システム内で自律的に動作を実行する能力を備えています。サイバーセキュリティの分野では、エージェントは脅威を検知した場合、IPアドレスをブロックしたり、データベースをシャットダウンしたりするなどの動作を自律的に行うことができます。最も重大なリスクは、「誤検知」によって自動応答がトリガーされ、大規模なサービス停止を引き起こす可能性があることです。
監査担当者は、「ガードレール」、「影響の大きいアクションに対するヒューマン・イン・ザ・ループ」による承認、およびエージェントが異常な動作をした場合にエージェントを停止させる「キルスイッチ」の存在を検証する必要があります。介入の削減（オプションB）は利点ではありますが、同時にこの運用リスクの主な要因でもあります。

質問: **87**
AIの利用規約における主な目的は次のうちどれですか？
A. AIの倫理的利用に関する指針の策定
B. AI利用状況監視手順の概要
C. 従業員に対し、AIツールの入手方法と使用方法について教育する
D. 異なる種類のAIの違いを説明する
正解: **A (**コメントを発表する**)**
AIの利用規約（AUP）は、組織内でAIツールやテクノロジーを倫理的かつ責任ある方法で使用する方法を定めたものです。AAIA™学習ガイドによると、AUPの主な目的は、不正使用を防止し、倫理的、法的、および運用上の基準の遵守を促進することです。
「AIの許容使用ポリシーは、AIツールの使用方法、特にデータ処理、公平性、および禁止されている使用方法に関するガバナンスを提供します。これは、従業員の行動を組織の価値観およびコンプライアンス要件に合致させるものです。」監視手順（B）、トレーニング（C）、および分類体系の説明（D）は、より広範なAIドキュメントに含まれる場合がありますが、AUPの中核的な目的は、倫理的な使用に関するガバナンスです。

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に関するポリシー、標準、倫理的枠組み」

質問: **88**
IS監査担当者がAIモデルを使用してワークシートを要約しているが、いくつかのワークシートには、モデルに統制上の不備を無視するように指示する「隠しセル」が含まれていた。リスクを最も効果的に軽減できる解決策はどれか？
A. モデルにデータ内の指示を無視して高温を設定するように指示します。
B. ワークシート内の定義済みの値とヘッダーのみを抽出します。
C. 変更履歴付き読み取り専用モードが有効になっていることを確認してください。
D. AIモデルにアップロードする前にファイルをPDFに変換します。
正解: **B** (コメントを発表する)
これは「データに基づくプロンプトインジェクション」であり、AIがデータを命令として扱います。監査担当者は「事前定義された値とヘッダーのみを抽出対象とする」ことで、AIの「コンテキストウィンドウ」を特定の既知のデータフィールドに限定します。これにより、AIが他のセルに隠された悪意のあるコマンドを「読み取り」て実行することを防ぎます。
高温（オプションA）では、モデルが不規則な指示に従う可能性が高くなるだけです。
PDFへの変換（オプションD）は効果的ではありません。なぜなら、最新のAIモデルはPDF内の隠されたテキスト層を読み取ることができるからです。

質問: **89**
AIソリューションを導入するかどうかを決定する際に、最も重要な考慮事項は次のうちどれですか？
A. AI導入のスピード
B. AI導入コスト
C. AIの倫理的意味合い
D. AIハードウェアに必要なスペース
正解: (正解を表示します)

質問: **90**
IS監査担当者が、トランザクションデータを格納する新しいデータベースの監査を計画するために、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すか？
A. データベースデータ変更における職務分掌の衝突の特定
B. アーキテクチャ図の作成
C. 技術固有のリスクと考慮事項の特定
D. データベース管理者（DBA）とのインタビューから得られた会議議事録の要約
正解: (正解を表示します)
生成型AIは、大規模なデータセットや技術文書を統合して、理解しやすい洞察を生み出すことに優れています。

AAIA™学習ガイドでは、複雑な環境を分析し、業界のリスクパターンと関連付けることで、ドメイン固有のリスクと管理上の考慮事項を特定するために、生成型AIを活用することを推奨しています。
「AIは、監査対象技術に合わせたリスクプロファイルを生成することで、監査計画段階で監査担当者を支援し、監査の焦点と範囲の優先順位付けに役立ちます。」インタビューの要約（D）や図の作成（B）は役立ちますが、実用的な情報で監査計画に直接役立つのはCだけです。A（職務分掌）は、後段階の統制評価です。
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：「計画とスコープ設定における生成型AIの活用」

質問: **91**
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示す。AIの最大の利点は、「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異常な挙動を特定できる点にある。AIは、悪意のある行為（ファイル名の急速な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出できる。このような事前検出は、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ある。
攻撃者を特定すること（オプションC）やリソースを節約すること（オプションD）も役立ちますが、セキュリティの中核となる価値は、AIを活用した異常分析によって提供される強化された検出機能にあります。

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　**275**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **92**
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。
B. 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。
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、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。
正解: **C** (コメントを発表する)

質問: **93**
AIの利用に関わる以下の内部脅威のうち、最も大きなリスクとなるのはどれでしょうか？
A. システムハイパーパラメータの漏洩
B. ソーシャルエンジニアリング攻撃の実施
C. システムバックアップの削除
D. 機密データの抽出
正解: (正解を表示します)
最大の内部脅威は、機密データの流出（D）です。AIシステムには、個人情報、財務情報、運用情報、専有情報など、豊富なデータセットが含まれていることがよくあります。内部関係者がこれらのデータを抽出したり漏洩したりすると、深刻な法的、規制上の、そして評判上の問題が発生する可能性があります。
バックアップの破壊（C）は可用性に影響しますが、機密性には影響しません。ソーシャルエンジニアリング攻撃（B）は深刻ですが、間接的な影響です。ハイパーパラメータの漏洩（A）はモデル構成を露呈しますが、通常は機密データを直接危険にさらすことはありません。AAIAは、データ機密性リスクがAIガバナンスにおいて最も深刻なカテゴリであることを強調しています。
参考文献：
ISACA、AAIA試験内容概要 - ドメイン5：倫理的および法的リスク、データ保護および機密保持。

質問: **94**
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: (正解を表示します)

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: **95**
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. データの層別化
B. システムの隔離
C. データのクリーニング
D. システムのトレーニング
正解: **C** (コメントを発表する)
データクレンジングは、AI開発ライフサイクルにおける基礎的な作業です。AAIA™学習ガイドでは、データ品質（完全性、正確性、一貫性、妥当性を確保すること）が、効果的で偏りのないAIシステムを構築する上で不可欠であると指摘しています。データクレンジングには、重複データの削除、エラーの修正、欠損値の処理、フォーマットの標準化などが含まれます。
「データクリーニングは、効果的なトレーニングと評価の前提条件です。質の低いデータは、不正確または誤解を招くモデル出力につながり、運用上および倫理上のリスクを高めます。」トレーニング（D）は不可欠ですが、データが適切に準備された後にのみ実施する必要があります。層別化（A）は特定のモデリング手法をサポートしますが、データの整合性に比べれば二次的なものです。したがって、データ収集段階ではCが最も重要なタスクとなります。
参考資料：ISACA Advanced in AI Audit™ (AAIA™) 学習ガイド、セクション：「AIの基礎と技術」、サブセクション：「データ収集と準備」

質問: **96**
深層学習ニューラルネットワークにおいて、人間の意思決定を模倣するために特徴抽出を行うため、IS監査人が評価する上で最も重要な層は次のうちどれでしょうか？
A. ハイパーパラメータ
B. 隠し

C. 入力
D. 出力
正解: **(**正解を表示します**)**
ニューラルネットワークにおいて、 隠れ層」とは、実際の変換と特徴抽出が行われる層です。これらの層は入力層と出力層の間に位置し、重み付けされた接続を通してデータを処理することで複雑なパターンを識別します。情報システム監査担当者にとって、隠れ層の評価は非常に重要です。なぜなら、隠れ層は人間の認知を模倣するモデルの 論理」を表しているからです。入力層と出力層は透過的ですが、隠れ層は解釈可能性に欠けることが多く、隠れたバイアスや非決定的な挙動のリスクにつながります。
これらの層の深さと活性化関数を理解することで、監査担当者はモデルの複雑さとエラーに対する脆弱性を評価するのに役立ちます。

質問: **97**
情報システム監査担当者が、ある組織が求人応募者の選考にAIを使用しているかどうかの監査を計画している。
監査範囲に含めるべき最も重要な項目は次のうちどれですか？
A. 候補者評価に使用されたデータの情報源
B. 選考されなかった候補者のデータを保持する
C. 組織内における過去の採用動向
D. AIモデルの詳細なコードレビュー
正解: **A (**コメントを発表する**)**
採用AIにおいて、出力の完全性と公平性は、ほぼ完全に 使用されるデータソース」に依存します。トレーニングデータが人間の偏見（例えば、特定の大学や性別からの採用のみ）を含む過去の記録から取得されている場合、AIはその偏見をコード化して自動化します。ISACA AAIA™マニュアルでは、 データソース」と データリネージ」を監査することが、アルゴリズムによる差別の根本原因を特定する最も効果的な方法であると述べています。データ保持 オプションB）は一般的なプライバシー上の懸念事項ではありますが、データソースに内在する偏った意思決定による重大なリスクに比べれば二次的なものです。

質問: **98**
IS監査担当者は、保険会社が使用しているAIベースの不正検出システムが、類似のケースを処理する際に一貫性のない結果を生み出すことに気づきました。監査担当者が推奨する最も効率的な対策は次のうちどれですか？
A. すべての意思決定に人間が関与する仕組みを導入する。
B. トレーニングデータとモデル評価パラメータを分析します。
C. AIシステムに対するユーザーアクセス制御と認証を強化する。
D. AIアルゴリズムを定期的に更新して、一貫性を向上させます。
正解: **B (**コメントを発表する**)**

類似のケースで結果が一致しない場合は、「モデルの安定性」または「データ品質」に問題がある可能性が高いです。最も効果的な対策は、「トレーニングデータとモデル評価パラメータを分析」して、モデルが偏ったデータセット、ノイズの多いデータセット、または代表性のないデータセットでトレーニングされたかどうかを特定することです。また、ハイパーパラメータの調整が不十分なために、入力のわずかな変化に対してモデルが不規則に反応してしまうことも、結果の不一致の原因となる可能性があります。人間が介入する（オプションA）ことで安全策は講じられますが、リソースを大量に消費し、根本原因に対処するものではありません。データとパラメータを調査することで、組織はモデルの根本的なロジックを修正し、長期的な一貫性を確保することができます。

質問: **99**
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. 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。
B. 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。
C. 経営陣はイノベーションの文化を推進する。
D. 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。
正解: **A** (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: **100**
IS監査担当者が、過去のデータに基づいたAIモデルが「データ遅延」を引き起こし、リアルタイムの意思決定の質を低下させていることを特定しました。以下のうち、最も適切な対策はどれですか？
A. データの多様性を検証する。
B. 特徴量の重み更新を実行します。
C. 利用可能なテストデータの量を増やす。
D. データソースが信頼できるものであることを確認します。
正解: (正解を表示します)

「データ遅延」は、モデルが現在の現実を反映しなくなった古いパターン（例えば、パンデミック以前の買い物習慣）に過度に依存している場合に発生します。これを軽減するために、「特徴量重み更新」を使用して、最新のデータポイントに高い重要度を与え、古いデータの影響を「減衰」させます。これにより、モデルはゼロから完全に再構築することなく、現実世界の変化に迅速に適応できます。データの多様性と量は一般的なパフォーマンスにとって重要ですが、重み調整のように時間的な「遅延」の問題に特に対処するものではありません。

質問: **101**
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**)**

質問: **102**
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。
虚偽表示は、監査の信頼性、規制遵守、および組織の意思決定を損なうため、リスクが高い。書式の不整合（C）と一般的な表現（D）は、見た目の問題です。古い情報（A）は懸念事項ではありますが、必ずしも誤った結論を導き出すものではありません。
幻覚に基づく誤情報は、AIが生成する監査報告書において最も深刻かつ危険な問題である。
参考文献：
AAIAドメイン3：監査プロセスにおけるAI（AI出力の正確性、幻覚リスク）。
AAIAドメイン5：AI支援作業における倫理的責任。

質問: **103**
データ処理における機械学習（ML）の主な目的は以下のとおりです。
A. AIモデルの出力の説明可能性を高める。
B. 人工人間知能を構築するための統計的推論を行う。
C. 通常、人間の知能を必要とする行動を実行する。
D. データセットを分析して、視覚的なパターンと傾向を特定します。
正解: **C** (コメントを発表する)

質問: **104**
高リスク環境で稼働するAIシステムに定期的なソフトウェアアップデートを適用する最も重要な理由は次のうちどれですか？
A. AIを利用したゼロデイ攻撃からシステムを保護する
B. モデルの学習サイクルを加速し、処理速度を向上させる
C. モデル出力に対する人的監視の必要性を低減するため
D. 脆弱性に対処し、出力整合性攻撃のリスクを軽減する
正解: (正解を表示します)
医療、金融、航空といった高リスク環境では、ソフトウェアのアップデートによって脆弱性が修正され、新たな攻撃経路に対処し、整合性制御が常に最新の状態に保たれることが保証されます。
AAIAは、旧式のAIシステムが以下の脆弱性を抱えていることを指摘しています。
* 完全性攻撃
中毒
* モデル回避
* 敵対的攻撃定期的なアップデートにより、AIソフトウェアとそれを支えるインフラストラクチャの両方が回復力を維持します。ゼロデイ攻撃対策（A）は要因の一つですが、主な理由ではありません。スピードと監視の軽減（BとC）は、リスクに基づく正当な理由ではありません。主な目的は、出力の完全性を維持し、AIの悪用を防ぐことです。
参考文献：
AAIAドメイン2：AI運用、パッチ管理、および整合性制御。

質問: **105**
継続的な改善を確実にするためのAIインシデント管理プロセスにおいて、最も重要なステップは次のうちどれですか？
A. 所有権を定義する
B. 根本原因分析
C. アーカイブログ
D. 重症度を評価する
正解: (正解を表示します)
根本原因分析（オプションB）は、継続的な改善において最も重要なステップです。なぜなら、インシデントが解決されるだけでなく、再発も防止されることを保証するからです。

AAIAのインシデント管理では、以下の点を重視しています。
* 根本的なシステム障害の特定
* 問題がデータ、モデルロジック、ドリフト、統合、または人的要因に起因するかどうかを判断する
長期的な緩和戦略の実施
ガバナンスと運用管理の更新
所有権（A）を明確にすることは、プロセスの早い段階で重要です。
重症度（D）を評価することで、対応の優先順位が決まります。
ログのアーカイブ（C）はドキュメント作成をサポートします。
しかし、これらのどれも、プロセス学習や長期的な回復力を保証するものではない。
根本原因分析は、組織の成熟とリスク低減にとって不可欠なステップである。
参考文献：
AAIAドメイン2：インシデント管理と事後レビュー
AAIAドメイン1：AIガバナンスの継続的改善

質問: **106**
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　**275**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **107**
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るでしょうか？
A. 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。
B. データドリフトがシステム予測に与える影響
C. 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

D. 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
正解: **B** (コメントを発表する)

質問: **108**
以下のうち、開発者がモデルに挿入する前に、バランス調整のための数値データを正しく解釈および識別していることを最初に保証するものはどれですか？
A. データ辞書
B. データ計算ライブラリ
C. 統計概要
D. 混同行列
正解: (正解を表示します)
Adata辞書(A)は、以下の内容を理解するための信頼できる情報源です。
* データ型と数値形式
* 有効な範囲と解釈
* フィールドの定義とビジネス上の意味
* 正規化とスケーリングに関する期待値
データのバランス調整や前処理を行う前に、開発者は各機能を正しく理解していることを確認する必要があります。
AAIAフレームワークは、数値変数の誤った解釈がしばしば以下のような結果を招くことを強調している。
* 正規化が正しくありません
* スケーリングの不具合
* 偏ったクラスバランス
* モデルのトレーニングが不正確
統計的要約（C）は分布の特定に役立ちますが、意味を検証することはできません。混同行列（D）は学習後に使用されます。ライブラリ（B）はツールであり、解釈の源ではありません。
参考文献：
AAIAドメイン2：データ管理 - データ辞書、メタデータ、データ理解

質問: **109**
組織のAIシステム向けデータガバナンスプログラムにおいて、成熟した効果的なアプローチを示す最適な指標は、以下のどの指標でしょうか？
A. 前会計年度中に完了したAIプロジェクトの数
B. データ系統が文書化されているAIモデルの割合
C. 組織のデータセットに対するデータ品質監査の頻度
D. 全部門におけるAI関連事業に割り当てられた総予算
正解: (正解を表示します)
文書化されたデータリネージ（オプションB）は、成熟したデータガバナンスの基盤となります。ISACA AAIA™学習ガイドでは、「AIのための効果的なデータガバナンスは、組織がデータのライフサイクル全体およびAIモデル内でのデータの発生源、変換、および使用を追

跡し、文書化できる能力によって特徴づけられる」と強調しています。この文書化は、透明性を提供し、説明責任を支え、効果的なリスク管理を可能にします。
定期的なデータ品質監査（オプションC）は重要ですが、それだけでは透明性やトレーサビリティを保証するものではありません。プロジェクト数（オプションA）や予算配分（オプションD）は、ガバナンスの成熟度を直接示す指標ではありません。
参考資料：ISACA Advanced in AI Audit™ (AAIA™) 学習ガイド、セクション：AIにおけるデータガバナンス：データリネージとトレーサビリティ」

質問: **110**
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. スコープクリープ
B. 計画コストの増加
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**)**

質問: **111**
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. 同意が適切に管理されていません。
B. 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。
C. 計算規模のトレーニングは実施されませんでした。
D. ハイパーパラメータは最適化されていません。
正解: **(**正解を表示します**)**
不正検出AIシステムにおける誤検出は、多くの場合、最適化されていないハイパーパラメータに起因する。
ハイパーパラメータは、学習率、判定閾値、複雑度ペナルティなど、モデルの学習プロセスにおける様々な側面を制御します。これらのパラメータが適切に調整されていないと、モデルが過敏になり、正常な動作を不審なものとして検出してしまう可能性があり、顧客からの苦情につながる恐れがあります。
「ハイパーパラメータの調整は、AIモデルにおける感度と特異度のバランスを取るために不可欠です。不適切な調整は、特に微妙なパターン認識を必要とする不正検出などのシステムにおいて、偽陽性または偽陰性の発生率を高める可能性があります。」オプションAとBはデータガバナンスに関連していますが、予測における偽陽性を直接引き起こすものではありません。オプションC（計算規模のトレーニング）は、モデルの精度ではなく効率に影響を与える可能性があります。したがって、Dが最も適切な回答です。

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：「モデルのチューニングと最適化」

質問: **112**
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。
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、効果はあるものの、包括的で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: **113**
IS監査担当者が、ある組織がセキュリティ目的でAI顔認識技術を使用していることを知りました。この慣行に関して、最も重大な倫理的問題は次のうちどれでしょうか？
A. 顔認識データへのアクセス制御の実施の難しさ
B. 特定の人口統計グループに対する潜在的な偏見
C. 生体認証セキュリティにおけるAI利用に関する国際標準の欠如
D. 個人がより慎重に交流し始める
正解: **(**正解を表示します**)**
ISACA AAIA™ 学習ガイドによると、顔認識システムは公平性とバイアスに関連する重大な倫理的リスクを抱えやすい。これらのシステムは、代表性のないトレーニングデータセットのために、特定の人口統計グループ（特に人種、性別、年齢に基づく）に対して高いエ

ラー率を示すことが多い。情報システム監査人にとって、これは重大なコンプライアンスおよび評判リスクとなる。なぜなら、バイアスのかかった結果は、差別的なアクセスや虚偽の告発につながる可能性があるからである。データセキュリティ（オプション A）と標準の欠如（オプション C）は関連性があるが、AI ガバナンスにおける根本的な倫理的責務は、生体認証アプリケーションが保護対象グループに不均衡な不利益を与えないようにすることである。

質問: **114**
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: **115**
異常検知機能が不十分なAIシステムを導入することに伴う最大のリスクは、次のうちどれですか？
A. 一貫性のないAIシステム構成管理
B. AIの意思決定の質に影響を与える、検出されないデータ汚染
C. AIモデルのドリフトに対するインシデント対応の遅延
D. AI報告基準への不遵守
正解: **B (**コメントを発表する**)**
異常検知が効果的でないということは、システムがデータやモデルの動作における異常なパターンを認識できないことを意味します。最大の危険は、データ汚染（B）が検出されないことであり、これはデータの完全性を損ない、AIの意思決定が破損、偏向、または安全でな

い結果につながります。AAIAは、異常検知は改ざん、データドリフト、または悪意のある操作を特定するために不可欠であることを強調しています。
構成の不整合（A）は運用上の問題ではありますが、被害ははるかに軽微です。ドリフト応答の遅延（C）はパフォーマンスの低下を引き起こす可能性がありますが、検出されないままのポイズニングほど深刻ではありません。報告基準の不備（D）はコンプライアンス上のリスクであり、意思決定の整合性が損なわれるほど重大な問題ではありません。
したがって、検出されない中毒は、モデルの信頼性と安全性に直接的な影響を与えるため、最も高いリスクをもたらす。
参考文献：
ISACA、AAIA試験内容概要 - ドメイン2：AI運用、AIにおける脅威と脆弱性。

質問: **116**
IS監査担当者が、会社のAI手順をレビューしています。以下のうち、最も重要なギャップはどれでしょうか？
A. 外部データソースの使用については規定されていません。
B. 重要システムに必要な必須評価は規定されていません。
C. AI手順においてプライバシー原則は定義されていません。
D. 人的監視の手順は記載されていません。
正解: **B** (コメントを発表する)
AIガバナンスには、リスクに基づいた「階層型アプローチ」が必要です。最も深刻な課題は、影響力の大きいシステムや重要なシステムに対する「義務的な評価」（バイアス評価やプライバシー影響評価など）が欠如していることです。これらの評価は、安全でない、あるいは倫理に反するAIの導入を防ぐ「制御ゲート」となります。プライバシー原則（オプションC）と監視（オプションD）は不可欠な要素ですが、これらは通常、リスク評価プロセスの結果として得られるものです。システムを稼働させる前に評価する義務がなければ、組織は他のAI制御策が最も必要とされる場所で確実に適用されていることを確認する手段がありません。

質問: **117**
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: **118**
以下のデータ管理方法のうち、AIモデルの相関関係の信頼性に最も大きなリスクをもたらすのはどれですか？
A. ソースデータから5パーセンタイルと95パーセンタイルの範囲外にある外れ値データ値を削除する
B. カテゴリ変数を数値形式およびエンコーディングに変換する
C. 取引合計金額のデータ型をオブジェクトから整数に変更
D. レコード内のすべての属性が一致するため、重複エントリを削除します
正解: **(**正解を表示します**)**
外れ値を除去することでモデルのパフォーマンスが向上する場合もありますが、「外れ値データの値を恣意的に削除する」ことは、正確なパターン認識に不可欠な、まれではあるものの正当なデータポイントを削除してしまう可能性があるため、信頼性に最も大きなリスクをもたらします。不正検出やリスク管理などの分野では、外れ値は最も重要なデータです。データの自然な分布を歪めると、相関関係が偏り、影響の大きい「テール」イベントを認識できないモデルになってしまう可能性があります。エンコード（オプションB）と真の重複データの削除（オプションD）は、標準的でリスクの低い前処理手順です。データ型の修正（オプションC）は、数学演算を可能にするために不可欠であり、リスクではありません。

質問: **119**
IS監査担当者が、トランザクションデータを格納する新しいデータベースの監査を計画するために、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すか？
A. 技術固有のリスクと考慮事項の特定
B. データベース管理者（DBA）とのインタビューから得られた会議議事録の要約
C. データベースデータ変更における職務分掌の衝突の特定
D. アーキテクチャ図の作成
正解: **(**正解を表示します**)**

質問: **120**
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: **121**
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るでしょうか？
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、実世界の入力データがトレーニングデータのパターンからずれると、AIシステムのパフォーマンス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、ドリフトを監視することが不可欠です。」トレーニングの多様性（A）と外れ値検出（D）は精度に関係しますが、トレーニングデータとリアルタイムデータの時間的なずれに対処しているのはBだけです。過学習（C）は、他の状況では汎化性能の低下を引き起こす可能性が高いでしょう。
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：「モデルの監視とデータドリフトの検出」

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　275問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **122**
IS監査担当者が大学で使用されているデータセットをレビューしています。モデルがすべてのデータを処理して必要な相関関係を算出できないリスクを最も示唆しているのは、次のうちどれでしょうか？
A. 学生番号フィールド（整数形式）
B. 学年レベルフィールド（float形式）
C. オブジェクト形式の最終成績パーセントフィールド
D. ブール形式の学士号を取得していること
正解: **(**正解を表示します**)**
機械学習において、「データ型」は基礎となるものです。数値フィールド（例えば、成績パーセント）が「オブジェクト」（文字列/テキスト）として格納されている場合、AIモデルは相関や平均の計算といった数学演算を実行できません。AAIA™マニュアルによると、これは「データ品質」の欠陥であり、「特徴量除外」につながります。つまり、モデルは変数を単純に無視するか、各数値を個別のテキストラベルとして扱い、定量的な意味をすべて失ってしまうのです。その他の形式（整数、浮動小数点数、ブール値）は、それぞれのデータ型に適しています。

質問: **123**
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: **124**

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. 出力結果を表示するダッシュボードを作成する。

B. 定期的なモデル監査レポートを提供する。

C. 文書の出典とデータ処理。

D. モデルの決定を説明するツールを使用する。

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　**275**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」