

以下はAWS認定AIプラクティショナー試験の直前レビュー用ノートです。

重要項目を体系的に整理し、試験対策の視点とセルフチェック項目を併記しています。

1. AI／機械学習／ディープラーニングの基礎

1.1 概念の整理

- **AI(人工知能)**: 人間の知的行動を模倣する広義の技術領域
- **機械学習(ML)**: データから学習して性能向上を目指す手法
- **ディープラーニング(DL)**: 多層ニューラルネットワークを用いるMLの一分野

1.2 主な学習手法

- 教師あり学習: ラベル付きデータで分類・回帰を実行
- 教師なし学習: ラベルなしデータでクラスタリングや次元削減を実行
- 強化学習: 環境との試行錯誤による報酬フィードバックで最適行動を習得

1.3 重要用語

用語	定義
パラメータ	<u>学習中</u> にモデルが更新する重みやバイアスなどの値
ハイパーパラメータ	<u>学習前</u> に設定しチューニング対象となる学習率などの値

試験対策

- AI・ML・DLの位置関係と特徴を自分の言葉で説明できるようにする
- 教師あり／なし／強化学習の代表的ユースケースを押さえる

教師あり学習: 顧客離反予測、画像分類

教師なし学習: 顧客セグメンテーション、異常検知

強化学習: ロボティクス、自律走行車

セルフチェック

- パラメータとハイパーパラメータの違いを例を挙げて説明できるか確認
-

2. AWS主要AIサービスとユースケース

2.1 サービス一覧と代表的用途

- **Amazon Rekognition**: 画像・動画の顔認識、物体やシーンのラベル検出、コンテンツモデレーション(不適切コンテンツ検出)
- **Amazon Comprehend**: テキストの感情分析、キーフレーズ抽出、トピックモデリング
- **Amazon Lex**: テキスト/音声によるチャットボット構築
- **Amazon Polly**: テキスト読み上げ(TTS)
- **Amazon SageMaker**: データ準備からモデル構築・トレーニング・デプロイまで
- **Amazon Bedrock**: 基盤モデル呼び出し、ファインチューニング、エージェント実行

2.2 サービス選択の着眼点

- 機能適合性: 要件に対して専門特化サービスか汎用プラットフォームか
- 運用負荷: サーバレス推論/マネージド型 vs. 自前インフラ管理
- セキュリティ・統合: VPC 統合、IAM ポリシー、バケットポリシーの適用可否

試験対策

- シナリオ問題を想定し、要件に合致するサービス選択理由を短文でまとめる
- 各サービスの誤選択肢パターン(別領域サービスの過誤)を覚える

セルフチェック

- 各サービスを一言で説明できる

- 誤選択肢を2つ挙げ、なぜ不適切か説明できる

3. Amazon SageMaker の理解と利活用

3.1 主な構成要素

1. **Notebook** インスタンス: VPC 内プライベートサブネット、最小権限 IAM ロール設定
2. **Training Job**: マネージドトレーニング、ハイパーパラメータ自動チューニング
3. **Endpoint**: リアルタイム／サーバレス／マルチモデル推論オプション
4. **Clarify**: バイアス検出、特徴量の重要度可視化
5. **Ground Truth**: 人手＋自動ラベリングによるデータセット作成

3.2 セキュリティ設定

- **VPC** エンドポイント: Notebook／Endpoint への通信をプライベート化
- **セキュリティグループ**: 必要最小限のポート・IP 制限
- **S3** バケットポリシー: 特定 IAM ロールのみアクセス許可

試験対策

- 各デプロイ方式(サーバレス vs. リアルタイム)の特徴と適用シナリオを図示
- セキュリティ設定手順をフローチャートで整理

セルフチェック

- Notebook のセキュリティ要件と設定方法を説明できる
- Endpoint タイプごとの使い分け理由を4文以内でまとめる

4. モデル評価と推論パラメータ

4.1 モデル評価指標

- 定量評価: 精度、再現率、F1 スコア、ROC-AUC
- 定性評価: 人間による評価 (創造性・文脈理解)、自動指標の限界把握

4.2 推論パラメータ調整

- 温度 (Temperature): 低温度→出力一貫性↑、高温度→創造性↑
- Top-K / Top-p: 生成候補の範囲制御による多様性調整

試験対策

- 各評価指標の適用ケースを例示 (不均衡データ→ROC-AUC)
- 推論パラメータの効果を短文で説明できるように練習

セルフチェック

- Temperature、Top-K、Top-p の違いと適用シーンを説明できる
- 定量 vs. 定性評価の使い分け例を2つ挙げる

5. 生成AI／LLM 応用技術

5.1 適応手法とトレードオフ

手法	特徴	コスト	性能向上度
インコンテキスト学習	プロンプト調整のみで適応	低	中
Few-shot Learning	少数例示でタスク適応	低～中	中～高
ファインチューニング	モデル再学習により分野特化	中～高	高
RAG (検索拡張生成)	外部知識ベース(ドキュメント等)を検索・参照し、回答の最新性と正確性を向上	中	高

試験対策

- コスト・開発工数・性能の観点で最適手法を選択するロジックを整理

セルフチェック

- 各手法の長所・短所を3行以内で比較説明できる
-

6. プロンプトエンジニアリング

6.1 基本アプローチ

- タスク分割: 複雑タスクを具体的サブタスクに分割
- **Chain-of-Thought**: 推論過程を明示化し精度向上
- プロンプトバージョン管理: 変更履歴を追跡し最適版を特定

試験対策

- タスク分割の有効性を例示し、言語化できるようにする
- CoT 活用シナリオを2例そろえて覚える

セルフチェック

- 実際のシナリオでどのアプローチを選ぶかを説明できる
-

7. 責任あるAI／倫理的考慮

7.1 原則と対策

原則	対策例
公平性	多様性があり、偏りのない代表的なデータセットの構築・検証
説明可能性	SageMaker Clarify による特徴重要度可視化
プライバシー	差分プライバシーの適用、暗号化

堅牢性 アドバーサリアルテスト、耐障害設計

試験対策

- 各原則に対応するAWSサービス・機能をセットで覚える

セルフチェック

- 原則と対策例を3セット書き出す

8. セキュリティ・コンプライアンス・ガバナンス

8.1 ネットワークとアクセス管理

- VPCエンドポイント + プライベートサブネット
- セキュリティグループでポート/IP 制限
- IAMロールの最小権限適用
- S3バケットポリシーによるアクセス制御

8.2 監視とログ

- CloudTrailのAPI呼び出しログをCloudWatch Logsで集中管理・監視
- Bedrock モデル呼び出しログの活用

8.3 コンプライアンス対応

- GDPR、HIPAA、SOC 2 など業界規制
- AWS Artifact で証明書／レポート取得

試験対策

- シナリオ問題で設定手順を即答できるよう演習

セルフチェック

- ネットワーク構成図とIAMポリシー例を自分で描いてみる
-

最後に

- 重要箇所は声に出して説明できるまで繰り返す
- 模擬試験で時間配分の練習を行う
- 試験前日は無理に詰め込まず、全体をざっと復習

以上のノートを繰り返し確認し、合格を目指してくださいね。