金融AIを支える
データ基盤の設計と構築



— セキュリティ・品質・ガバナンスを両立する実践ガイド —

金融AIの高度化には、「モデル」より先に「データ基盤」が必要

勘定系・情報系・外部データ・文書が分散したままでは、AIは判断根拠を示せず、PoCから本番運用へ移行できない。
本資料は、金融機関がAIを実運用に載せるためのデータ基盤要件を、設計・品質・セキュリティ・ガバナンスの観点から体系化する。

Start影hallenge影onsulting影o.,駄d.
2026年8月 発行 ／ 第1版

Confidential ／ 社外への再配布・二次利用を禁じます

本資料の目的と対象読者

金融AI活用の障壁は、モデルの性能ではなくデータの供給体制にある。本資料は、要件定義からガバナンスまでの設計論点を、金融業務の単位で整理する。

本資料の目的

金融AIの活用に必要なデータ基盤の要件を、業務・技術・統制の観点で体系化する

PoCから本番運用へ移行するための前提条件を明示する

個別ツールの選定ではなく、設計判断の順序と論点を示す

本資料で分かること

データ分散・定義不統一を解消する手順

収集・蓄積・整備・活用の各層の設計選択肢

品質・セキュリティ・ガバナンスの実装観点

導入ロードマップと推進体制の組み方

対象読者

機関 銀行・信用金庫・保険・証券・カード・リース等

部門 経営企画、DX推進、IT企画、データ分析、リスク管理、システム部門

想定するAI活用領域

法人融資提案
与信審査
不正検知
顧客提案・チャネル最適化
RAGによる社内照会回答
市場リスク分析

本資料の読み進め方

① P3–P5：現状課題の構造化と、AI活用から逆算した基盤要件の定義
② P6–P12：アーキテクチャ、連携・蓄積・統合、品質、セキュリティの設計
③ P13–P18：ガバナンス、規制・監査対応、運用、導入ロードマップと推進体制

注記｜本資料は設計論点の整理を目的とし、特定の金融機関の実測値・製品評価は含まない。／提案：自機関の状況に読み替えたうえで、P18のチェックリストで着手可否を判断する。

金融AI活用を阻むデータ基盤の課題

データの分散と定義の不統一が、AIの根拠提示と本番移行を阻む。PoC停滞の原因は技術的性能ではなく、データの所在・定義・責任が未整備であることに帰着する。

発生事象	直接原因	構造的原因	業務への影響	経営への影響
PoCでは動いたAIが本番運用に移行できない	勘定系・情報系・外部サービスにデータが分散している	顧客・商品・取引の定義が部門ごとに異なる	抽出・突合の手作業が残り、分析と判断が遅延する	AI投資がPoC止まりとなり、効果を計上できない
分析に必要なデータの抽出が、都度の個別依頼になる	紙・PDF・音声・メールなど非構造化データが増加している	データ品質とオーナーシップの責任が定義されていない	AI出力を人が検証できず、利用範囲が限定される	規制対応・監査説明のコストが継続的に増加する
AI出力の根拠を業務部門に提示できない	データの所在・責任者・更新時刻が分からない	セキュリティ・利用可否の判断が案件ごとの個別対応	同一顧客の重複・誤認が営業と審査の双方に波及する	説明責任を負えず、重要業務へのAI適用を判断できない
同じ指標が部門ごとに異なる値で報告される	連携が個別開発の積み上げになっている	基盤への投資が業務効果と結び付いていない	監査・照会対応に都度の調査工数が発生する	競合との顧客提案力・審査スピードの差が固定化する

注記 | 解釈：課題は「発生事象」ではなく構造的原因（定義・責任・統制の未整備）に起因する。／提案：着手優先度は経営への影響が大きい領域から逆算して決定する。本ページに実測値は含まない。

金融AIに求められるデータの全体像

必要なデータは顧客・取引・外部・非構造化の4系統に整理できる。加えて学習用・推論用・評価用を分けて管理することが、精度検証と説明責任の前提となる。

① 顧客・契約データ

個人・法人の属性情報、法人番号、業種、規模

口座、契約、限度、保証・担保情報

同意状況、利用目的、チャネル登録情報

主な所在：勘定系、CRM、契約管理

② 取引データ

入出金、決済、カード利用、為替

融資実行・返済、延滞、条件変更

投資・運用、ポジション、残高推移

主な所在：勘定系、決済系、証券系

③ 外部データ

市場データ（価格、金利、指数、時系列）

企業情報、決算、業界統計、ニュース

信用情報、制裁・反社チェック情報

留意：契約条件・利用範囲・提供継続性

④ 非構造化データ

面談記録、稟議書、審査メモ

契約書、規程、マニュアル、通達

通話録音、メール、チャット、帳票PDF

留意：版管理と閲覧権限の継承が必須

⑤ AI用途別データ

学習用　過去実績と結果ラベル。期間と抽出条件を固定

推論用　判断時点で取得できる最新データのみ

評価用　学習に使わない検証データと正解

用途別データを分ける理由

学習時に「判断後に判明した情報」が混入すると、検証では高精度でも本番で再現しない。判断時点で取得可能なデータのみを推論用として定義し、評価用は学習から完全に分離する。

注記 | 解釈：データ整備の優先順位は「量」ではなく、AI活用領域が要求する系統の網羅性で決まる。／提案：4系統ごとに所在・責任者・更新頻度を棚卸ししたうえで、用途別の区分を定義する。

AI活用から逆算する基盤要件

基盤要件は活用領域ごとに異なる。「すべてをリアルタイムに統合する」のではなく、領域別に必要な鮮度・精度・説明性の水準を定義することが投資効率を左右する。

AI活用領域	必要なデータ	基盤に求められる要件	設計上の主な論点
法人融資提案	財務諸表、取引履歴、面談記録、業界情報	正確性、説明可能性	出所・更新時刻の記録、提案根拠となる文書への追跡
与信審査	顧客属性、返済履歴、信用情報、資金使途	最新性、公平性	更新頻度の定義、属性による偏りの検証と記録
不正検知	決済明細、端末・ログイン情報、行動履歴	リアルタイム性	ストリーミング連携、低遅延での特徴量供給と再現性
顧客提案	商品・契約情報、チャネル接点、応答履歴	顧客単位の統合	名寄せ・MDM、同意と利用目的の範囲管理
RAG・照会回答	規程、マニュアル、通達、FAQ、契約雛形	検索精度、版管理	版・有効期限・閲覧権限の継承、根拠の提示方法
市場リスク分析	市場価格、金利、ポジション、評価前提	時系列整合性	基準時刻の統一、遡及修正の履歴保持と再計算

要件定義の順序

① 活用領域を選定 → ② 必要データと所在を特定 → ③ 鮮度・精度・説明性の水準を合意 → ④ 基盤要件（連携方式・保持期間・権限）へ落とす

注記｜解釈：領域ごとに要件が異なるため、全社一律の高水準要件は過剰投資となる。／提案：初期対象は要件が単純で説明責任が明確な領域（例：社内照会回答）から選定する。

金融AIデータ基盤の全体アーキテクチャ

基盤は6層に分離する。層を分けることで、上流システムの変更をAI活用層に波及させず、再処理と監査証跡の起点を固定できる。

① データソース　勘定系・情報系・CRM・決済・市場データ・文書／音声

▼

② 連携・取り込み　API・ETL／ELT・ファイル連携・CDC・ストリーミング

▼

③ 蓄積・統合　データレイク／DWH／データマート（レイクハウス構成を含む）

▼

④ 整備・管理　品質管理・データカタログ・権限管理・リネージュ・マスキング

▼

⑤ AI活用層　機械学習モデル・生成AI・RAG・特徴量／プロンプト管理

▼

⑥ 業務チャネル　審査・営業支援・照会対応・モニタリング・報告

処理方式の使い分け

バッチ：日次の残高・実績集計、モデル再学習
マイクロバッチ：時間単位の状況把握、督促・照会
ストリーミング：不正検知・与信の即時判定

配置形態の選択

オンプレミス：勘定系近接、機密性の高い原本
クラウド：分析・生成AIの拡張性と調達速度
ハイブリッド：境界・持ち出し制御を明文化

層を分離する目的

上流の仕様変更をAI活用層に波及させない
再処理・切り戻しの起点を層単位で固定する
監査時に説明すべきデータフローを単純化する

注記 | 解釈：層の分離は技術要件ではなく、変更管理と説明責任のための統制設計である。／提案：初期構築では③④を最小構成で確立し、⑤以降を段階的に追加する。

データ収集・連携方式の設計

連携方式は「必要な鮮度」と「勘定系への負荷」という2つの制約で決まる。全件抽出を前提にせず、差分取得（CDC）と再処理可能性を設計初期に織り込む。

連携方式	特性	適した用途	留意点
API連携	必要時に少量を取得。疎結合を保てる	照会、単票参照、外部データ	大量一括取得には不向き。流量制御と障害時の再試行設計が必要
ETL／ELT	まとめて抽出・加工。ELTは変換を基盤側で実施	日次集計、分析用データ整備	加工ロジックの所在が分散しやすい。変換定義の版管理を必須とする
ファイル連携	既存の帳票・媒体授受を踏襲できる	レガシー連携、外部機関授受	到着遅延・欠損の検知が遅れやすい。件数・ハッシュによる突合を実装
CDC（差分取得）	更新差分のみを取得。元システム負荷が小さい	勘定系マスタ・取引の準リアルタイム反映	削除・遡及修正の扱いを明確化。初期同期と差分の整合確認が必要
ストリーミング	発生イベントを逐次流す。低遅延	不正検知、即時アラート	重複配信・順序逆転の前提設計（冪等処理）が不可欠

勘定系への負荷を抑える取得

全件再取得ではなく差分取得を基本とする
抽出はオンライン時間帯を避け、複製環境から取得する
加工処理は基盤側で行い、元システムに持ち込まない
同一データを複数経路で重複取得しない

外部データ利用時の確認事項

契約上の利用範囲（AI学習利用の可否、再配布制限）
提供元の品質保証水準と改定・停止時の通知条件
提供継続性のリスクと代替ソースの確保
取得目的と自機関の利用目的の整合性

連携失敗時の再処理と欠損検知

到着予定時刻を定義し、未着・遅延を自動検知する
件数・金額合計・ハッシュで送受信を突合する
同一処理の再実行で結果が変わらない設計とする
欠損期間中のAI出力を利用停止とする条件を定める

注記｜解釈：連携方式の選択誤りは、鮮度不足ではなく元システム負荷と再処理不能として現れる。／提案：方式はデータ単位で選択し、一覧化して合意する。

データレイク・DWH・データマートの設計

原本を改変せずに保管し、共通定義への統合と用途別の提供を分離する。Raw／Standardized／Curatedの3層管理が、再処理と監査説明の前提となる。

Raw層｜データレイク：取得した原本をそのまま保管する

構造化データの抽出結果、PDF・画像・音声・メールなど非構造化データの原本を無加工で保持する
取得元・取得時刻・対象期間・実行ジョブをメタデータとして必ず付与する
加工後に誤りが判明した場合、この層から再処理できることが要件（原本を上書き・削除しない）
保持期間は業務・規制上の要請から個別に定義し、期限到来時の削除手続きを自動化する

▼

Standardized層｜DWH：全社共通の定義に統合する

顧客・法人・商品・取引の定義を統一し、コード体系・単位・通貨・基準時刻を揃える
名寄せ結果、履歴（有効開始／終了日）、削除フラグを保持し、過去時点の再現を可能にする
ここで定義した項目名と意味をデータカタログに登録し、部門間の呼称差異を解消する
変換ロジックはコードとして版管理し、いつ・誰が・なぜ変更したかを追跡できる状態に保つ

▼

Curated層｜データマート：用途別に整形して提供する

融資・営業・リスク・不正検知など、業務単位で必要項目に絞ったデータセットを提供する
AI用途では学習用／推論用／評価用を別データセットとして明示的に切り出す
参照可能な部門・役割をデータセット単位で設定し、個人情報はマスキング後に提供する
利用実績を記録し、参照されないマートは統廃合の対象とする（乱立の防止）

レイクハウスを採用する場合

レイクとDWHを単一基盤に統合し、原本と統合データを同じ管理下に置く構成

利点：非構造化データとの併用が容易、重複コピーの削減、権限管理の一元化

留意：3層の論理的な区分は維持する。物理統合を「層の区分が不要」と誤解すると、加工前後の切り分けが失われ、再処理と監査説明が困難になる

避けるべき状態

原本を上書きし、取得時点の状態に戻せない

統合層を経由せず、各部門が直接レイクから独自加工する（定義の再分裂）

用途別マートが無管理に増殖し、同一指標に複数の値が並存する

誰がどのデータを参照しているか把握できない

注記｜解釈：3層管理の目的はストレージ最適化ではなく、原因追跡と再処理の担保である。／提案：物理構成（レイクハウス採用の有無）に関わらず、3層の論理区分は維持する。

顧客・企業・取引データの統合

顧客単位の統合はAI活用の前提だが、誤った名寄せは営業・審査の双方に誤判断を波及させる。自動判定と人による確認を分離し、判定根拠を記録する運用が必要となる。

① 識別子の名寄せ

顧客ID：システムごとに異なる採番を統合IDへ紐付ける
法人番号：法人の一次識別子として活用し、商号変更に追随する
口座番号：統廃合・支店統合による変更履歴を保持する
照合キー：氏名・住所・生年月日・電話番号の正規化（表記統一）を前処理として実施する

② 関係性の管理

法人と代表者・役員・保証人の関係
親会社・子会社・関連会社のグループ構造
グループ与信・与信集中の把握に必要な出資関係
取引関係（仕入先・販売先）の把握範囲
関係の成立日・解消日を保持し、時点指定で参照できる状態にする

③ マスターデータ管理（MDM）

正となるマスタ（顧客・法人・商品・組織）を1つに定める
項目ごとに「どのシステムの値を優先するか」を決定ルールとして明文化する
登録・変更・統合・分離の申請と承認の手続きを定義する
マスタ変更を下流システムへ伝搬する仕組みを持つ

④ 有効期間と履歴管理

属性値ごとに有効開始日・終了日を保持し、上書きしない
「審査時点の顧客状態」を再現できることが、AI判断の説明責任の前提となる
データ発生時刻と基盤反映時刻を区別して保持する
遡及修正は履歴として追加し、修正前の値も参照可能とする

名寄せの誤りが招くリスク

過剰統合（別人を同一と判定）
他人の取引情報が閲覧され、個人情報の目的外提供に該当しうる。与信判断も誤る

統合漏れ（同一を別人と判定）
与信集中を検知できず、顧客単位の残高・リスクを過小評価する

誤統合を抑える運用

確度に応じて「自動統合」「保留（人が確認）」「非統合」に区分する
統合の判定根拠（一致した項目・スコア）を記録する
誤統合が判明した場合の分離手続きと、下流への訂正伝搬を用意する
保留件数と誤りの発生状況を定期的に報告する

注記 | 解釈：名寄せは精度100%を前提にできないため、誤りを検知・訂正する運用込みで設計する。／提案：自動統合の閾値は、業務影響の大きさから業務部門と合意して決定する。

非構造化データとRAG基盤

RAGの品質は生成モデルではなく、文書の版管理・権限継承・根拠提示の設計で決まる。旧版や閲覧権限外の文書が検索対象に残ることが、金融実務での最大のリスクとなる。

① 取り込み

対象：規程・通達・マニュアル、稟議書、契約書、面談記録、帳票PDF、通話録音

原本を改変せず保管し、文書管理システム上の識別子と紐付ける

② テキスト化・付帯情報

OCR（表・押印・手書きの認識精度を事前検証）
音声認識（話者分離、専門用語辞書）

メタデータ付与：文書種別、所管部署、版、制定・改定日、有効期限、機密区分

③ 分割・ベクトル化

条・項の構造を保持した文書分割（機械的な文字数分割は根拠提示を困難にする）

Embedding生成、ベクトル検索と全文検索の併用、章立てを用いた絞り込み

④ 検索・回答生成

利用者の権限で参照できる範囲のみを検索対象とする

回答には出典（文書名・版・該当箇所）を必ず併記し、原文へ遷移できる状態にする

⑤ 業務利用

照会対応、審査補助、契約チェック、研修

回答の採否は利用者が判断する前提とし、質問・回答・出典を記録して品質改善に用いる

版・有効期限・閲覧権限の継承

改定時に旧版を検索対象から除外し、現行版のみを回答に用いる（改定の反映遅れが誤回答の主要因）
廃止・失効した規程は削除ではなく「無効」として保持し、過去回答の検証に備える
文書管理システム上の閲覧権限を、ベクトルデータと検索結果に継承する
権限変更・文書削除を検索索引へ反映する時間差を定義し、監視対象とする
過去時点の回答を再現できるよう、参照した版と索引の状態を記録する

機密情報の除外と「回答できない」の制御

取り込み前に機密区分を判定し、対象外文書を索引に登録しない（登録後の除外は漏れが生じやすい）
個人情報を含む箇所はマスキング・仮名化した上で索引化する
検索結果の関連度が閾値を下回る場合は回答せず、担当部署への照会を案内する
根拠文書を提示できない場合は回答を生成しない設計とする
回答禁止領域（法令解釈、個別与信の可否判断など）を明示的に定義する

設計上の要点

RAGの精度改善は、モデル変更より「文書側の整備（版管理・構造化・メタデータ付与）」の効果が大きい。導入時は対象文書を限定し、所管部署が改定を反映できる運用を先に確立する。

注記 | 解釈：金融実務での主要リスクは生成内容の誤りより、旧版・権限外文書の参照である。／提案：初期対象は所管が明確で改定頻度の管理された規程類から選定する。

データ品質管理の設計

品質は「良い／悪い」ではなく、項目ごとの許容値として定義する。AI出力の誤りを入力データまで遡って検証できる状態が、業務適用の可否判断を支える。

品質観点	確認内容	許容値の設定例（要合意）	AIへの影響
完全性	必須項目の欠損、連携件数の不足	重要項目の欠損率を業務ごとに上限設定	欠損の多い属性に依存したモデルは本番で判定不能となる
正確性	原本との一致、コード値の妥当性、桁・単位	残高・金額は原本と完全一致（差異ゼロ）	誤った学習データは、検証で気付けない継続的な誤判定を生む
一貫性	システム間の値の不整合、定義・基準時刻の相違	主要指標の突合差異は原則ゼロ、例外は理由を登録	部門により同じ指標で異なる値が出て、AI出力の信頼を損なう
適時性	到着遅延、反映遅れ、基準時点からの経過	用途別に到着期限を定義（例：日次処理は始業前）	古いデータでの推論は、最新性を要件とする与信・不正検知で致命的
重複性	同一取引の二重計上、顧客の重複登録	重複検知件数を監視し、未処理残を上限管理	残高・与信集中を過大／過小に評価する

品質ルールと自動検知

項目単位に検査ルール（必須、型、範囲、コード一覧、相関）を定義する
取り込み時に自動検査し、閾値超過を検知した時点で下流処理を停止する
異常値・形式不一致・重複は隔離領域へ退避し、原因調査後に再投入する
検知結果を品質スコアとして時系列で記録し、劣化傾向を把握する

データリネージュによる原因追跡

項目レベルで「どのソースから、どの変換を経て生成されたか」を記録する
異常検知時に影響を受ける下流のマート・モデル・帳票を特定できる
定義変更の影響範囲を事前に評価できる
監査時に、報告数値の生成経路を提示できる

AI出力の誤りを遡って確認する仕組み

推論時に使用した入力データ（値・時点・出所）を出力と併せて保存する
誤りの原因を「データ品質」「モデル」「利用方法」に切り分けて判定する
データ起因と判定した場合、品質ルールを追加して再発を防ぐ
誤り事例を評価用データセットに追加し、次回検証に反映する

注記｜表中の許容値は設定の考え方を示す例（仮定値）であり、実際の水準は業務影響から個別に合意する。／解釈：品質管理の目的はAI誤出力の原因切り分けを可能にすることにある。

セキュリティとアクセス制御

AI活用では、権限管理に加えて「入力データと生成結果の持ち出し制御」が新たな統制対象となる。既存の情報管理規程を、AI利用の経路まで拡張して適用する必要がある。

① 暗号化と環境分離

保存時：ストレージ・DB・バックアップ・ベクトルデータの暗号化。鍵の管理主体と交換手続きを定義する
通信時：システム間・外部連携・利用者端末との通信を暗号化し、経路を限定する
環境分離：開発・検証・本番を分離し、権限・ネットワーク・運用者を別管理とする
検証環境へ本番データを持ち込む場合は、マスキング・仮名化を必須とし、承認と期限を設定する
生成AI／外部サービス利用時は、送信先・送信データ・保持期間を事前に評価する

② 権限管理（RBAC／ABAC）

RBAC（役割ベース） 役職・職務に応じて参照範囲を付与する。管理が単純で監査説明が容易
ABAC（属性ベース） 部店・担当顧客・機密区分・時間帯などの属性で動的に判定する。細粒度の制御に適する

行・列単位の制御（担当外顧客の非表示、機密項目の非開示）を基盤側で実装する
権限は最小限から付与し、定期的な棚卸しと自動失効を設ける
特権IDは常用せず、申請・承認・期限・操作記録を必須とする

③ 個人情報の加工と操作記録

マスキング：表示・出力時に一部を隠す。用途に応じて項目単位で設定する
仮名化：識別子を置換し、対応表を分離管理する（復元可能性を統制下に置く）
匿名化：個人を識別できない状態に加工する。復元しない前提で利用範囲を定める

操作・参照・出力ログを保存し、大量参照や通常外の出力を検知する
ログの改ざん防止と保持期間を定義し、監査時に提示できる状態を維持する

④ AI利用における持ち出し制御

入力：AIへ送信可能なデータ区分を定義し、機密・個人情報の送信を技術的に制限する
学習利用：外部サービスにおける入力データの学習利用可否を契約で確認する
出力：生成結果のダウンロード・転送・外部共有を、区分に応じて制御する
記録：入力・出力・利用者・時刻を保存し、事後に検証できる状態にする
権限継承：AIが参照するデータは、利用者本人の権限範囲を超えないことを保証する
逸脱時：検知条件と利用停止の判断者、停止手順を事前に定める

注記｜解釈：AI経由の情報漏えいは、権限設定の不備よりも「権限のある利用者による出力の持ち出し」として生じやすい。／提案：入力・出力の両方向で制御と記録を設計する。

AIガバナンスとモデル管理

AIを業務に組み込む条件は、責任者が特定され、判断根拠が記録され、停止と切り戻しが実行できることである。この3点が満たされない領域には適用しない。

① 責任の明確化

データオーナー　定義・品質・利用可否の判断責任を負う（原則として業務部門）

モデルオーナー　精度・利用範囲・停止判断の責任を負う

いずれも部署ではなく役職単位で特定し、変更時の引継ぎ手続きを定める

② 学習データとモデル版の対応管理

モデル版ごとに、学習データの抽出条件・期間・件数・前処理を記録する
推論結果には、使用モデル版と入力データの時点を必ず付与する
特徴量の定義と生成コードを版管理し、学習時と推論時の差異を防ぐ
過去の判断を、当時のモデルとデータで再現できる状態を維持する
プロンプト・検索設定も生成AIの構成要素として版管理の対象に含める

③ バイアス・精度劣化・ドリフトの監視

バイアス：属性ごとの判定結果の偏りを定期的に検証し、記録する
精度劣化：正解が判明する業務（返済実績、不正確定）で継続的に実績評価する
ドリフト：入力データの分布変化を監視し、再学習の判断基準とする
監視指標と閾値、逸脱時の報告先を事前に定義する

④ 説明可能性と根拠の記録

顧客に不利益となりうる判断では、根拠を業務用語で提示できることを要件とする
影響の大きい要因、参照した文書（RAG）、閾値との関係を記録する
「説明可能性」の水準は用途ごとに定義する（内部検証用と顧客説明用は別要件）
モデル内部の説明手法に依存せず、業務判断として説明可能な形式に整える

⑤ Human in the Loop

AIの役割を「提示・下書き・優先順位付け」と「最終判断」に区分する
顧客への不利益判断、与信・謝絶、規制解釈は人の最終確認を必須とする
確認者が根拠を検証できる情報（出典・入力値）を画面上に提示する
人が修正した内容を記録し、モデル改善の入力とする

⑥ 利用停止・切り戻しの手順

停止の判断基準（精度低下、誤判定の重大性、データ欠損）を数値で定義する
判断者と連絡経路、停止操作の実施者を明確にする
旧モデル版へ切り戻す手順と、切り戻し後の妥当性確認を用意する
停止中の業務継続方法（人による代替処理）を併せて設計する
停止・再開の判断内容を記録し、事後に検証できる状態とする

注記｜解釈：ガバナンスはAI導入の制約ではなく、重要業務へ適用するための前提条件である。／提案：停止・切り戻し手順を整備できない領域では、AIを判断の補助に限定する。

金融規制・監査に対応する管理

監査で問われるのは技術構成ではなく、「誰が何を承認し、どの経路のデータで判断したか」を提示できるかである。証跡は事後に作成できないため、基盤要件として先に組み込む。

管理領域	主な確認事項	基盤側で用意すべきもの
個人情報・機密情報の管理	保有する個人情報の範囲、保管場所、加工状態、保持期間、削除の実施状況	項目単位の機密区分台帳、保管先の一覧、削除実行の記録
取得目的と利用目的の整合	取得時に示した目的の範囲内での利用か、AI学習利用が許容範囲か、同意の取得状況	データセット単位の利用目的・同意区分の登録、範囲外利用の技術的制限
委託先・クラウドの管理	委託先の選定・評価、再委託の把握、データ所在地、サービス停止時の対応、監査権の確保	利用サービス一覧と処理データの対応表、契約条件の管理、代替手段の整理
証跡・変更履歴・承認履歴	誰が何を変更・承認したか、変更前後の内容、参照・出力の記録、改ざん防止	定義・権限・モデル・プロンプトの変更履歴、承認記録、操作ログの長期保存
説明可能なデータフロー	報告数値・AI判断が、どのソースからどの加工を経て生成されたか	データカタログとリネージュ、レイヤー構成図、更新頻度と基準時刻の定義書

関連部門との連携の型

法務・コンプライアンス：利用目的の適合性、外部データの契約範囲、顧客説明の要否
リスク管理：モデルリスクの評価、影響度に応じた承認水準の設定
内部監査：統制の設計と運用状況の検証、証跡の十分性確認
連携の型：ユースケース単位で「事前評価 → 条件付き承認 → 運用開始後の定期報告」を定型化する
案件ごとの個別調整を繰り返さないため、判断基準と提出資料の様式を標準化する

監査対応で不足しやすい点

加工ロジックが個人の手元（表計算・スクリプト）に残り、経路を再現できない
モデル・プロンプトの変更が記録されず、過去の判断を検証できない
検証環境に本番データが残置され、権限管理の対象から外れている
外部サービスの利用実態が台帳と一致していない
削除・保持期間の定義があるが、実行された記録がない

注記｜本ページは一般的な管理観点の整理であり、適用される法令・監督指針の解釈は法務・コンプライアンス部門の判断による。／提案：要件は設計段階で確定し、構築後の追加対応を避ける。

運用監視と障害対応

AI基盤の障害は停止ではなく「誤った値で動き続ける」形で現れる。監視対象を稼働状況からデータ品質とAI出力品質へ拡張し、影響範囲を即時に特定できる状態を作る。

① 監視すべき対象

連携　到着遅延、処理停止、件数の欠損・急増
品質　欠損率、異常値、重複、突合差異
AI精度　実績との乖離、判定分布の変化、ドリフト
回答品質　根拠提示率、回答不能率、利用者評価
利用状況　参照件数、権限逸脱の試行、応答時間

② ダッシュボードの構成

運用担当向け：連携ジョブの成否、遅延、品質検査の結果
業務部門向け：データ更新時点、利用可否の状態、AI精度の推移
管理層向け：ユースケース別の利用実績と効果、重大インシデントの件数

閾値超過は表示のみでなく、責任者への通知経路を定義する

③ 障害発生時の影響範囲特定

リネージュから、影響を受けるマート・モデル・帳票・業務画面を特定する
影響期間（いつからいつまでのデータが不正確か）を確定する
当該期間のAI出力を「参考扱い」または「利用停止」とする判断を行う
業務部門への通知と、既に行われた判断の再確認の要否を決定する

④ 再処理・切り戻し・業務継続

再処理：Raw層から任意期間を再実行でき、結果が一意になる設計（冪等性）
切り戻し：データ・定義・モデルそれぞれの復旧手順と、復旧目標時間を定義する
業務継続：AI停止中の代替手段（人による処理、旧ルールベース）を用意する
復旧後：再処理結果の妥当性確認を経て、利用再開を承認する

⑤ 変更の影響管理

データ定義変更：影響する下流とモデルを事前評価し、周知期間を設ける
上流システム更改：連携仕様の変更をリネージュで洗い出す
モデル変更：旧版との判定差異を検証し、差異理由を記録する
規程改定：RAGの索引更新完了までの回答制御を定める

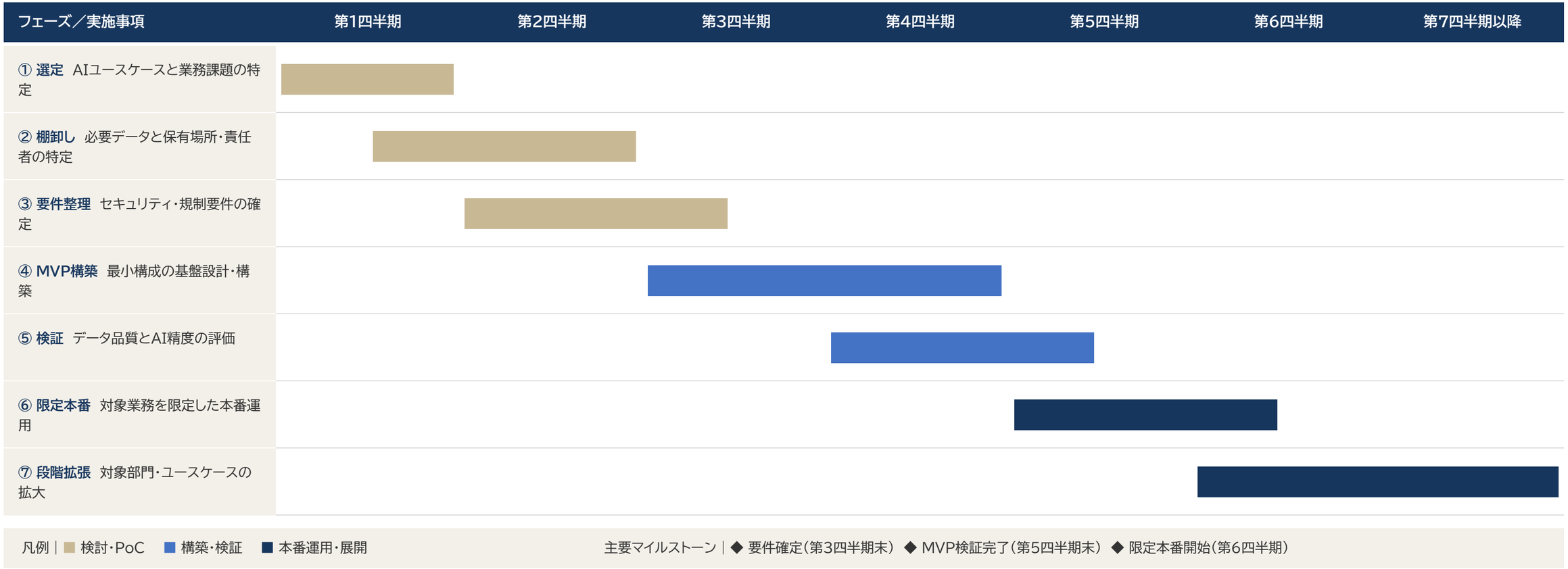
⑥ 問い合わせ・インシデント体制

一次受付を単一窓口に集約し、データ／モデル／業務の切り分けを行う
重大度の定義と、重大度別のエスカレーション先・報告期限を定める
AI出力への異議・誤り申告の受付経路を業務部門に明示する
インシデントは原因区分ごとに集計し、品質ルールと運用手順に反映する

注記｜解釈：AI基盤の運用リスクは「停止」より「誤った値での継続稼働」にある。／提案：稼働監視とデータ品質監視を同一のダッシュボードで扱い、責任者への通知条件を定義する。

導入ロードマップ

全社基盤を先に完成させる進め方は、投資回収の見通しが立たないまま長期化する。1ユースケースを本番運用まで通し、そこで確立した統制を横展開する順序が有効である。



全社基盤を最初から完成させない
初期構築は対象ユースケースが必要とするデータ範囲に限定する。統合対象を全データに広げると、要件合意に時間を要し効果検証に到達しない。

高価値・低リスク領域から着手する
判断基準：業務効果が測定可能／個人情報の関与が限定的／誤りを人が検証できる／所管部署が明確。社内照会回答や書類作成支援が該当しやすい。

注記｜図中の期間配分は標準的な進め方を示す想定（仮定値）であり、実際の期間は対象範囲・既存基盤の状況・体制により変動する。／提案：フェーズ④以降は前フェーズの検証結果を条件に着手判断する。

構築プロジェクトの体制と役割

データ基盤の構築はIT部門単独では完結しない。正解データの提供と利用可否の判断は業務・法務側の責任であり、役割を先に確定することが遅延を防ぐ最大の要因となる。

役割	主な責任	具体的な提供・判断事項	不在時に生じる問題
経営・事業責任者	目的、投資、リスク許容度の決定	対象ユースケースの優先順位、予算、AI適用範囲の承認	部門間の要件対立が解消せず、範囲が発散する
業務部門	要件・判断基準・正解データの提供	項目定義の確定、品質許容値の合意、評価用の正解付与、出力の検証	精度を評価できず、本番適用の可否を判断できない
IT・データ部門	基盤設計、連携、品質、運用	連携方式の選定、3層設計、品質検査の実装、監視と再処理の整備	個別開発が積み上がり、再処理・追跡が不能になる
AI開発部門	モデル・RAG・評価設計	特徴量設計、評価指標と検証方法、モデル版管理、再学習の判断	検証環境の高精度が本番で再現しない
セキュリティ部門	権限、ログ、脅威対策	権限方式の決定、暗号化・環境分離、ログ保存要件、持ち出し制御	構築後の指摘で設計変更が発生する
法務・リスク管理	規制、説明責任、利用可否判断	利用目的の適合性、外部データ契約の確認、顧客説明の要否、モデルリスク評価	運用直前に利用不可と判明し、投資が回収できない
内部監査	統制状況と証跡の確認	統制の設計・運用状況の検証、証跡の十分性の確認	証跡を事後に再構成できず、説明が困難になる

推進上の要点

役割は部署単位ではなく役職単位で特定し、意思決定の期限を設定する。業務部門の関与工数（正解データ提供・出力検証）を計画に明示的に織り込む。

典型的な失敗パターン

IT部門主導で構築を進め、業務部門の要件確定と法務判断が後追いとなる。結果として、完成後に利用範囲が縮小され効果を計上できない。

注記｜解釈：構築遅延の主要因は技術課題ではなく、判断者不在による意思決定の停滞である。／提案：フェーズ開始前に各役割の担当者名と決定期限を文書化して合意する。

設計前チェックリストとまとめ

以下10項目に未確定の事項が残る状態で構築に着手すると、PoC後の本番移行段階で設計の手戻りが生じる。着手前に責任者と合意しておくべき論点として整理する。

設計前チェック（10項目）

- ☐ **目的・KPI** AIで解決する業務課題と、達成を測る指標が定義されているか
- ☐ **データ特定** 必要なデータ項目と取得元システムを具体的に特定できているか
- ☐ **責任者** データ項目ごとの責任者（データオーナー）が役職単位で決まっているか
- ☐ **品質基準** 品質の許容値と更新頻度・到着期限を業務部門と合意しているか
- ☐ **情報分類** 個人情報・機密情報を項目単位で分類し、加工方針を定めているか
- ☐ **権限設計** 参照範囲を業務・役割単位で設計し、AI経由の参照にも適用できるか
- ☐ **根拠の記録** AIの判断根拠（入力値・参照文書・モデル版）を記録できるか
- ☐ **人の確認** 人が最終確認すべき判断の範囲を明確にしているか
- ☐ **停止・切り戻し** 障害・誤判定時に利用停止と切り戻しを実行できるか
- ☐ **運用・コスト** PoC後の本番運用体制と継続コストを見積もっているか

本資料の要点（再掲）

要件はAI活用領域から逆算する
必要な鮮度・精度・説明性は領域ごとに異なる。全社一律の高水準要件は過剰投資となる（P5）

層の分離が再処理と説明を担保する
Raw／Standardized／Curatedの区分は、原因追跡と監査説明のための統制設計である（P6・P8）

RAGの品質は文書側の整備で決まる
版管理・権限継承・根拠提示が、旧版参照と権限外参照を防ぐ（P10）

停止できないAIは適用しない
責任者の特定・根拠の記録・停止と切り戻しの3点が、重要業務への適用条件となる（P13）

まとめ

金融AIの信頼性は、モデル性能だけでは決まらない。正確で安全なデータを継続的に供給し、利用履歴と判断根拠を説明できるデータ基盤を持つことが、金融AIを実運用へ移行させるための条件である。

注記｜提案：本チェックリストをユースケース単位で適用し、未確定項目が残る場合は着手範囲を縮小するか、当該項目の決定を先行させる。

お問い合わせ

本資料の内容に関するご相談、自機関の状況に即したデータ基盤の要件整理・設計支援については、下記までお問い合わせください。

Start Challenge
Consulting co., ltd.
挑む力が、世界を照らす

Start Challenge Consulting co., ltd.

会社名	Start Challenge Consulting co., ltd.
担当	平出
お問い合わせ先	info@startchg.com
ご相談内容	AIユースケースの選定、必要データの棚卸し、基盤要件の整理、 品質・セキュリティ・ガバナンス設計、導入ロードマップの策定

挑む力が、世界を照らす

金融AIの実運用化は、モデルの選定ではなくデータ基盤の整備から始まります。着手範囲の見極めから運用体制の設計まで、貴機関の状況に応じてご支援します。

Confidential ／ 本資料の無断転載・二次利用を禁じます。