

## 1 セキュリティ要件

★**データ分類ポリシー** Public/Internal/Confidential/Restrictedの定義を渡す。LLMへ出してよい情報の境界が固定され、機密漏えいと過剰な伏せ字の両方を防ぐ

★**AI利用ガイドライン** LLM入力可否の範囲とプロンプトインジェクション対策を渡す。生成物の扱いと禁止入力が明確になり、社内規程違反の出力を抑える

★**情報セキュリティ基本方針** ISMS規程を版数つきで渡す。提案や設計が自社のセキュリティ前提と矛盾せず、後工程の手戻りが減る

認証・認可方式 IdP/SAML/OIDC/MFAの採用方式を渡す。認証回りの実装案が既存基盤に乗る形に揃う

暗号化要件 保存時/通信時の暗号化、KMSと鍵管理方針を渡す。鍵の置き場や方式の食い違いを設計段階で潰せる

ネットワーク要件 閉域・Private Link・IP許可リストの前提を渡す。到達不能な構成案や許可外の経路提案を避けられる

ログ・監査要件 保存期間・改ざん防止・PII除外の方針を渡す。監査に通るログ設計が初手から出る

データレジデンシー要件 国内保管やリージョン縛りを渡す。越境保存になる構成提案を未然に弾ける

脆弱性対応プロセス SBOM・CVE対応SLA・ペネトレ方針を渡す。依存追加やパッチ提案が運用ルールに沿う

## 2 コーディング規約・開発標準

★**Lintor/Formatter設定現物** ESLint/Prettier/Ruff/Biome等の実ファイルを渡す。スタイル指摘が言葉でなく実設定で揃い、生成コードが即CIを通る

★**言語/FW/ランタイム版数縛り** EOLを跨がない版数指定を渡す。古い構文や非対応APIを使った提案が出なくなる

★**Git運用ルール** ブランチ戦略・コミット規約・PRテンプレを渡す。コミット文やPR説明が社内様式で生成される

★**セキュアコーディング規約** OWASP Top 10やIPA講座に沿う社内規約を渡す。入力検証やエスケープ漏れを生成段階で防ぐ

## データ分類×AI入力可否

| ランク | 名称                       |
|-----|--------------------------|
| L0  | 公開情報                     |
| L1  | 社内一般                     |
| L2  | 機微                       |
| L3  | 禁止（PII・原価・NDA・PCI-DSS対象） |

## Tips・補足

NGリスト（禁止ライブラリ・禁止クラウド・NG表現）をネガティブリストで持つと幻覚が減る

命名規則 変数/関数/DB/環境変数の命名規則を渡す。リネーム差し戻しが減る

ディレクトリ構成 feature-based/layer-basedの方針を渡す。ファイル配置が既存構造に揃う

エラーハンドリング/ログ出力方針 例外設計とログ粒度の方針を渡す。握りつぶしや過剰ログの提案を抑える

テスト方針 カバレッジ目標・テスト比率・テストデータ方針を渡す。テスト生成が運用ルールに沿う

## 3 アーキテクチャ・インフラ

★**クラウド利用サービスホワイトリスト** 採用可否を明示したサービス一覧を渡す。許可外サービス前提の構成案を弾ける

★**既存構成図/API仕様書/データモデル** C4 Modelやarc42形式の現物を渡す。接続点と責務が把握され、既存資産に接続する設計が出る

laC方針 Terraform/CDK/Bicepの採用方針を渡す。インフラコードが社内標準の書式に揃う

CI/CD標準 必須ステージ構成を渡す。パイプライン提案が既存ゲートを踏む形になる

API設計規約 Microsoft REST GuidelinesやGoogle AIPベースの規約を渡す。エンドポイント設計が一貫する

DB方針 RDBMS/NoSQL選定とスキーマ管理方針を渡す。マイグレーション運用に沿う案が出る

監視・オブザーバビリティ標準 OpenTelemetry等の計装方針を渡す。メトリクスとトレースの実装が標準に揃う

コンテナ/オーケストレーション コンテナ前提とオーケストレーション方針を渡す。実行環境に合う構成案になる

## 4 コンプライアンス・法務

★**業界規制** FISC・3省2ガイドライン・個人情報・GDPR等の適用範囲を渡す。規制に触れる処理やデータ移送の提案を未然に防ぐ

★**OSSライセンスポリシー** OSI/SPDXベースの許容と禁止ライセンス一覧を渡す。NGライセンス依存を生成段階で除外できる

契約上の制約 再委託・海外サーバー・権利帰属の制約を渡す。契約違反になる構成や外部送信を避けられる

監査要件 J-SOX・ITGC・内部統制の要件を渡す。統制に必要な証跡を残す設計になる

アクセシビリティ要件 JIS X 8341-3やWCAG 2.2の準拠レベルを渡す。コントラストや代替テキストを満たすUI案が出る

## 5 ビジネス・ドメイン

★**用語集** 業界・社内・略語の正式名と読みを渡す。独自語の取り違えが消え、出力の業務用語が正確になる

★**組織図/ステークホルダーマップ** RACI付きの体制図を渡す。誰の承認が要るかを踏まえた提案や文書が出る

業務フロー図 As-Is/To-BeをBPMN 2.0で渡す。現行業務に接続する改善案が出る

KPI/KGI/ビジネス目標/競合 数値目標と競合情報を渡す。施策提案が事業ゴールに紐づく

ペルソナ/ユーザージャーニー 想定利用者とユースケースを渡す。要件や画面案が利用文脈に沿う

## 6 プロジェクト運営

開発プロセス WF/アジャイル/SAFeのどれかを渡す。成果物の粒度とサイクルが運営に揃う

ドキュメンテーション標準 テンプレ現物を渡す。生成ドキュメントが社内様式で出る

意思決定プロセス RACIと承認フローを渡す。決裁経路を踏まえた進め方の提案になる

課題・チケット管理ルール 起票と分類のルールを渡す。タスク分解がチケット運用に沿う

## 7 運用・保守

SLA/SLO/SLI 目標値と指標定義を渡す。可用性前提に合う設計と監視案が出る

障害対応プロセス オンコールとポストモーテムの運用を渡す。障害時の手順や記録様式に沿う提案になる

バックアップ/DR RPO/RTOの目標を渡す。復旧目標を満たす構成案が出る

リリース・変更管理 CAB承認など変更フローを渡す。リリース手順が統制ルールに沿う

## 食わせる順序

1 **用語集** 社内・業界の略語と独自用語。取り違えの土台を最初に消す

2 **データ分類ポリシー+AI入力可否ルール** 渡してよい情報の境界を二番目に固定する

3 **既存システム構成図と接続点** 接続先と責務を渡し、既存資産に乗る設計を引き出す

4 **ステークホルダー・承認フロー** 決裁経路を渡し、進め方の提案を現実に合わせて

5 **Lintor/Formatter設定ファイル現物** スタイルを実設定で渡し、生成コードをCIに通す

6 **採用技術ホワイトリスト** 許可技術を渡し、許可外提案を弾く

7 **ドキュメントテンプレート現物** 様式を渡し、成果物の体裁を整える

## 格納先 振り分け

**AGENTS.md** 横断の最小公倍数。コーディング規約・テスト/ビルド手順・ディレクトリ構成。多くのツールが読む

**CLAUDE.md** Claude Code用。AGENTS.mdを@importで1ソース化。版数つき規約とNGリスト

**Claude Projects** 用語集・構成図・データモデルなど長文資料。フェーズ別に切替えて常時参照

**システムプロンプト** 役割・出力形式・トーン・絶対禁止事項などセッション固定の制約

**.cursor/rules** Cursor用.mdc。globsでファイル種別ごとにスコープ、Alwaysは最小限

**.github/** copilot-instructions.md。Copilotがリボ単位で自動付与、2ページ以内が目安

## Sources（公式・一次情報 / クリックで開く）

- OWASP Top 10 for LLM Applications 2025 — [genai.owasp.org/llm-top-10](https://www.owasp.org/llm-top-10)
- NIST AI Risk Management Framework 1.0 — [www.nist.gov/itl/ai-risk-management-framework](https://www.nist.gov/itl/ai-risk-management-framework)
- 経産省・総務省 AI事業者ガイドライン — [www.meti.go.jp/policy/it\\_policy/ai\\_guideline/index.html](https://www.meti.go.jp/policy/it_policy/ai_guideline/index.html)

- NIST SP 800-60 Vol.1 Rev.1 — [csrc.nist.gov/pubs/sp/800/60/v1/r1/final](https://csrc.nist.gov/pubs/sp/800/60/v1/r1/final)
- OWASP Top 10:2021（日本語） — [owasp.org/Top10/2021/ja](https://owasp.org/Top10/2021/ja)
- Conventional Commits v1.0.0 — [www.conventionalcommits.org/ja/v1.0.0](https://www.conventionalcommits.org/ja/v1.0.0)
- C4 Model — [c4model.com](https://c4model.com)

- Cursor Rules ドキュメント — [docs.cursor.com/context/rules](https://docs.cursor.com/context/rules)
- Claude Code メモリ（CLAUDE.md） — [docs.claude.com/en/docs/claude-code/memory](https://docs.claude.com/en/docs/claude-code/memory)
- GitHub Copilot リポジトリカスタム命令 — [docs.github.com/copilot/customizing-copilot/adding-repository-custom-instructions-for-github-copilot](https://docs.github.com/copilot/customizing-copilot/adding-repository-custom-instructions-for-github-copilot)

- AGENTS.md — [agents.md](https://agents.md)