

MUSUBI PLATFORM

課題管理表

Issue / Risk Register

要件定義書 v0.3 ・ 方式設計書 v0.2 から課題・未検討要素を集約（IPA準拠・多観点レビュー反映）

版数 v0.1（2026-06-29）

分類 セキュリティ/データ/運用/機能・事業/法令/UX・SEO

状態 済 / 対応中 / 未着手 ・ 影響：高 / 中 / 低

二重予約防止(advisory lock)・Webhook幕等・コアRLS定義は実装済み。本表は「その先の未対応」を管理する。

課題サマリ・運用方法

本表の位置づけ

- ・要件定義(検討漏れ・未決)と方式設計(技術課題)の論点を一元管理する受け皿。
- ・各課題に 分類・影響度・状態・対応方針 を付し、着手で対応中→済 に更新。
- ・短期(設計と不可分)から着手。済の根拠はコミット/構築ログに記録。

1

済

3

対応中

41

未着手

45

課題総数

最優先（短期・設計と不可分）：ISS-01 予約API防御／ISS-02 RLS分離テスト／ISS-09 レポート断面／ISS-10 予約数集計／ISS-18 TZ統一／ISS-24 課金⇔提供連動。
ISS-03(webhook認証スキップ)は本対応で済。

課題：セキュリティ・予約基盤

ID	課題内容 (対応方針)	影響	状態
ISS-01	公開予約APIの多層防御：レート制限/CAPTCHA/冪等キー/メール実在検証 (※二重予約はlock済)	高	未着手
ISS-02	RLSのテナント分離 自動テスト + reservationsのポリシー追加 (コアRLSは0002/0003/0007で定義済・2リポ分散)	高	未着手
ISS-03	/api/stripe/webhook の認証スキップ漏れ → middleware に skip 追加	高	済
ISS-04	監査ログ (予約/課金/公開削除/口コミ投稿の操作履歴・append-only)	中	未着手
ISS-05	シークレット運用：restricted key・**/*.env 一括ignore・ローテーション・CIスキャン	中	未着手
ISS-06	サブドメイン乗っ取り対策：削除のreconciliation (DNS ↔ Pages整合)	中	未着手
ISS-07	PII最小化・列暗号化(pgcrypto)・保持TTL/Storageの公開/非公開分離	中	未着手
ISS-08	メール認証：DMARC段階適用・ダブルオプトイン/MX検証・バウンス監視	中	未着手

課題：データ・アーキテクチャ

ID	課題内容（対応方針）	影響	状態
ISS-09	レポートの時系列スナップショット（MRR/前年比・upsert上書きで断面喪失を回避・追記型）	高	未着手
ISS-10	予約数のレポート集計是正：GA4イベント未実装のため reservations テーブルから集計	高	未着手
ISS-11	ホスト名による店舗識別の堅牢化：hostnameエイリアス表・正規化・未マッチ検知	高	未着手
ISS-12	在庫モデルの拡張：営業時間ルール+例外日+枠(slot)+リソース種別（席種/コース）	中	未着手
ISS-13	content(jsonb)の schema_version・投入バリデーション・テンプレ更新時の追従	中	未着手
ISS-14	外部IDの集約(store_integrations)・リード→ストアのID対応(lead_id)	中	未着手
ISS-15	ソフトデリート・参照整合(ON DELETE RESTRICT)・解約後のデータ保持/削除/エクスポート	中	未着手
ISS-16	マスタ化（プラン/席種/コース）・契約時価格スナップショット	低	未着手

課題：運用・信頼性（SRE）

ID	課題内容（対応方針）	影響	状態
ISS-17	SLO/RTO/RPO の数値化・PITR確保・復元演習（コンポーネント別）	高	未着手
ISS-18	タイムゾーン統一：UTC保存/JST境界（月次集計・予約日の境界）	高	未着手
ISS-19	Cron無音故障の死亡通知監視 + Stripe ↔ DBの日次突合（冪等の実装済）	中	未着手
ISS-20	デプロイ失敗のロールバック(Instant Rollback)・公開前確認・スモークテスト	中	未着手
ISS-21	バス係数1の解消：手順/台帳/全SaaSアクセスの2名共有・外部エスカレーション先	高	未着手
ISS-22	無料枠上限の監視と移行閾値・ログ集約/相関ID・保持期間	中	未着手
ISS-23	サポート/問い合わせ窓口・一次応答SLA（店主/来店客）	中	未着手

PRODUCT

課題：機能・課金・事業

ID	課題内容（対応方針）	影響	状態
ISS-24	課金⇄公開/予約/口コミの状態機械（自動連動）+ subscription系の幕等	高	未着手
ISS-25	課金の実テスト（契約→課金→失敗→解約）・料金表確定・未入金/領収書	中	対応中
ISS-26	来店客の予約変更/キャンセル/リマインド/No-show・予約状態機械	中	未着手
ISS-27	口コミ承認運用：★1～3は人手必須・期限切れは保留・承認代行オプション	中	未着手
ISS-28	Google Business Profile API 承認（口コミ取得/投稿の本番疎通・外部待ち）	高	対応中
ISS-29	オーナー自己編集・マルチユーザー権限境界（RLS）	中	未着手
ISS-30	解約オフボーディング・データ可搬性・サブドメイン回収/301	中	未着手
ISS-31	多店舗/チェーン対応（オーナーと店舗の分離・複数店切替・請求まとめ）	低	未着手

課題：法令・コンプライアンス

ID	課題内容 (対応方針)	影響	状態
ISS-33	個人情報の管理者/委託先の整理・DPA締結・越境移転の情報提供	高	未着手
ISS-34	電通法の外部送信規律：GA4等の外部送信ポリシー公表をテンプレ標準装備	高	未着手
ISS-35	営業メールのオプトイン(特電法)・配信停止/送信者表示・取引メールと系統分離	高	未着手
ISS-36	利用規約/サブスク約款/プライバシーポリシー/SLAの整備	高	未着手
ISS-37	制作物の表記責任分界(景表法/特商法/食品表示)・店舗の最終承認	中	未着手
ISS-38	予約者情報の保持期間・開示/削除請求窓口・要配慮情報(アレルギー)	中	未着手
ISS-32	独自ドメイン接続・ステージング環境	中	未着手

課題：公開サイト・予約UX・SEO

ID	課題内容（対応方針）	影響	状態
ISS-39	満席時の代替提示（近接日/別時間帯/電話導線）＝離脱防止	高	未着手
ISS-40	営業時間の単一ソース管理＋構造化データ(schema.org Restaurant)	高	未着手
ISS-41	重複コンテンツ対策：canonical固定・テンプレ/未公開はnoindex・sitemap自動	中	未着手
ISS-42	画像最適化/CWV(WebP/srcset/遅延/寸法)・モバイル追従CTA(電話/予約/地図)	高	未着手
ISS-43	予約フォーム検証/二重送信防止・確認/前日リマインドメール	高	未着手
ISS-44	予約カレンダーのa11y・コントラスト保証・alt入力	中	未着手
ISS-45	多言語(英＋hreflang)・OGP/SNSカード自動生成	低	未着手