VTO API Service

機能一覧リファレンス

ホスト型バーチャル試着 API / Widget サービス

https://asp.kitemir.jp/API/

Version 1.0 | 2026 年 4 月 6 日

Developer Reference

1. サービス概要

VTO API Service は、外部 EC サイトにバーチャル試着（Virtual Try-On）機能を提供するホスト型 API サービスです。<script> タグ 1 行の追加で、試着ボタン・モーダル UI・結果表示が動作します。

本番 URL	https://asp.kitemir.jp/API/
API ベース	https://asp.kitemir.jp/API/api/
認証方式	HMAC-SHA256 署名 + JWT トークン
VTO エンジン	FASHN AI v1.6 + OpenAI Vision（コメント生成）
決済	Stripe Billing（サブスクリプション）
Widget	JS + CSS 読み込みで即利用可 / CSS カラーカスタマイズ対応

2. 料金プラン

2 つの有料プランを提供しています。いずれも税別価格です。

項目	Starter	Pro
月額料金（税別）	¥5,500	¥16,500
対象	小〜中規模 EC サイト	大規模 EC サイト
VTO 実行回数/月	100 回	300 回
API キー発行数	最大 5 個	最大 5 個
Widget 方式対応	対応	対応
AI デザイナーコメント	対応	対応
カラーカスタマイズ	対応	対応
メールサポート	対応	対応
API 使用量分析	-	対応
優先サポート	-	対応
カスタム統合支援	-	対応

月間上限を超過した場合、追加リクエストは拒否されます（追加料金は発生しません）。プラン変更はいつでも可能で、翌月から新料金が適用されます。

3. 認証フロー（HMAC-SHA256 + JWT）

Widget 方式では、2 段階の認証を行います。

3.1 トークン取得フロー

Step 1: 客先サーバーのプロキシエンドポイントで HMAC 署名を生成

```
message = "api_key|origin|timestamp"
signature = HMAC-SHA256(message, shared_secret)
```

Step 2: token.php に POST → JWT トークンを取得

Step 3: Widget JS が Bearer JWT で VTO API を呼び出し

検証項目	詳細
HMAC 署名	api_key|origin|timestamp をパイプ結合し shared_secret で署名。hash_equals() で比較
タイムスタンプ	現在時刻との差が ±5 分（300 秒）以内であること
Origin 検証	primary_domain または allowed_domains（JSON 配列）に含まれること
JWT 有効期限	デフォルト 3600 秒（1 時間）/ HS256 アルゴリズム
JWT ペイロード	{ sub: user_id, origin, iat, exp }

4. API エンドポイント一覧

メソッド	エンドポイント	認証	説明
POST	/API/api/token.php	HMAC	JWT トークン発行
POST	/API/api/tryon.php	JWT	VTO 実行（人物画像+衣服画像）
GET	/API/api/status.php	JWT	VTO ステータスポーリング
GET	/API/api/verify.php	なし	API キー検証・残量確認
POST	/API/api/keys.php	Session	API キー生成・失効（最大 5 個）
POST	/API/api/update_domain.php	Session	ドメイン登録・更新
POST	/API/api/payment.php	Session	Stripe Checkout セッション作成
POST	/API/api/webhook.php	Stripe 署名	Stripe Webhook 受信
GET/POST	/API/api/dengonban.php	なし	伝言板 API（VTO 待ち時間用）

4.1 POST /API/api/token.php — JWT トークン発行

項目	内容
リクエスト	api_key, origin, timestamp, signature（HMAC-SHA256）
レスポンス	{ "success": true, "data": { "widget_token": "eyJ...", "expires_in": 3600 } }
検証内容	HMAC 署名・タイムスタンプ ±5 分・Origin ドメイン・サブスク有効性

4.2 POST /API/api/tryon.php — VTO 実行

項目	内容
認証	Authorization: Bearer {JWT}
リクエスト	person_image（file/base64）, garment_url（URL 文字列）, category（tops/bottoms/dresses）
Content-Type	multipart/form-data または application/json
レスポンス	{ "success": true, "data": { "tryon_id": "xxx", "status": "processing" } }
月間制限超過	HTTP 402 — Monthly VTO quota exceeded
コスト	$0.0750 USD / 1 回実行（FASHN AI 課金）

4.3 GET /API/api/status.php — ステータスポーリング

項目	内容
パラメータ	tryon_id={prediction_id}
認証	Authorization: Bearer {JWT}

処理中	{ "success": true, "data": { "status": "processing" } }
完了時	{ "success": true, "data": { "status": "completed", "result_url": "...", "designer_comment": "..." } }
ポーリング間隔	推奨 2 秒間隔 / 最大 60 回（2 分）でタイムアウト
AI コメント	完了時に OpenAI Vision API でデザイナーコメント自動生成（250-300 文字）

5. Widget 仕様

VtoWidget は、EC サイトに埋め込むためのフロントエンドコンポーネントです。JavaScript + CSS の 2 ファイルを読み込むだけで、試着ボタン・モーダル UI・結果表示が動作します。

5.1 読み込みコード

```
<script src="https://asp.kitemir.jp/API/widget/vto-widget.js"></script>
<link rel="stylesheet" href="https://asp.kitemir.jp/API/widget/vto-widget.css">
```

5.2 初期化

```
VtoWidget.init({
  tokenEndpoint: '/api/vto_token.php',   // 客先プロキシ
  apiBase: 'https://asp.kitemir.jp/API_SERVICES',
  colors: {
    primary: '#6C3483', accent: '#D4AC0D',
    primaryDark: '#4a2554', bg: '#FAF8F5'
  }
});
```

5.3 試着実行

```
VtoWidget.open({
  garmentUrl: 'https://example.com/product.webp',
  garmentUrls: [...],  // カラー別画像（最大 7 枚）
  category: 'tops',    // tops / bottoms / dresses
  productName: '商品名',
  productPrice: 12000,
  onAddToCart: function(selectedColor) { /* カート追加 */ }
});
```

5.4 Widget 機能一覧

機能	詳細
カラー選択 UI	garmentUrls で最大 7 色の衣服画像を切替。カラーセレクター UI を自動表示
人物画像アップロード	ファイル選択 + プレビュー表示。Canvas API で JPEG 変換・1500px 以下リサイズ
進捗表示	VTO 処理中のプログレスバー表示（実測 18-19 秒 / 表示「30-60 秒」）
ステータスポーリング	2 秒間隔で自動ポーリング。最大 60 回（2 分）でタイムアウト
デザイナーコメント	AI が試着結果を分析し、プロのファッションアドバイスを自動生成

カート連携	onAddToCart コールバックで選択カラー名を渡してカート追加
CSS カスタマイズ	CSS 変数方式 (--vto-primary 等) でブランドカラーに合わせた配色変更
レスポンシブモーダル	モバイル・デスクトップ対応。オーバーレイクリックでは閉じない (x ボタンのみ)
伝言板連携	VTO 処理待ち時間中に DengonbanWidget (ポストイット風メッセージボード) を表示

6. マイページ（ダッシュボード）機能

契約ユーザーは、Web ブラウザからマイページにログインして以下の機能を利用できます。

ページ	機能	詳細
ダッシュボード	サブスク状態表示	現在のプラン・月間実行数・残量をプログレスバーで表示
	API キー管理	キーの一覧表示・新規生成・失効（最大 5 個）・クリップボードコピー
	ドメイン設定	primary_domain（必須）+ allowed_domains（複数可）の登録・更新
	Shared Secret 表示	マスク表示 + 表示/非表示トグル。HMAC 署名に使用
料金・プラン	プラン比較表	Free / Starter / Pro の機能比較マトリックス
	プラン変更	Starter / Pro へのアップグレード・Stripe Customer Portal リンク
利用状況	当月利用状況	実行数 / 上限・プログレスバー・残量表示・80%/100%警告
	6 ヶ月チャート	Chart.js 折れ線グラフで過去 6 ヶ月の利用推移を可視化

7. 認証・会員管理機能

機能	詳細
会員登録	メール・パスワード・会社名・担当者名・ドメイン。メール認証トークン送信
メール認証	トークンリンクで認証。認証完了まで API 利用不可
ログイン	メール + パスワード（bcrypt）。セッションキー: api_user_id
パスワードリセット	メールでリセットトークン送信 → 新パスワード設定
セッション管理	PHP セッション。asp_user_id とは別キー（衝突防止）

8. Stripe Webhook 処理

metadata.service === 'api_service' で EC Suite の Webhook と判別します。

イベント	処理内容
`checkout.session.completed`	サブスクリプション有効化 + API キー自動生成 + ライセンス通知メール送信
`customer.subscription.updated`	ステータス更新（active/past_due/canceled）・期間更新・プラン変

	更検知
`customer.subscription.deleted`	サブスクリプションを canceled にマーク
`invoice.payment_failed`	ステータスを past_due に設定

9. エラーコード一覧

HTTP コード	意味	対処法
200	成功 / API レベルエラー	success=false の場合は message フィールドを確認
400	Bad Request	必須パラメータの不足・不正な値
402	Payment Required	月間 VTO 実行回数の上限超過。プランアップグレードが必要
403	Forbidden	JWT 無効・HMAC 不一致・Origin 不正・サブスク無効
404	Not Found	指定した prediction_id が存在しない
405	Method Not Allowed	HTTP メソッドが不正 (GET/POST の指定ミス)
429	Too Many Requests	レートリミット超過 (伝言板: 60 秒間隔)

10. データベーステーブル (api_ プレフィックス)

テーブル	主要カラム・用途
`api_plans`	id, name, stripe_price_id, price_jpy, max_vto_per_month
`api_users`	email, company_name, primary_domain, allowed_domains(JSON), shared_secret, stripe_customer_id
`api_keys`	user_id, api_key(api_XXXX-XXXX-XXXX-XXXX), name, status(active/revoked)
`api_subscriptions`	user_id(UNIQUE), plan_id, stripe_subscription_id, status, current_period_end
`api_usage_logs`	user_id, month_year(YYYY-MM), count — UNIQUE 制約(user_id, month_year)
`api_vto_executions`	prediction_id(UNIQUE), category, status, result_url, designer_comment, cost_usd
`api_cost_logs`	month_year(UNIQUE), total_count, total_usd — 月間コスト集計

11. 公開ページ一覧

ページ	内容
`pages/index.php`	ランディングページ (サービス紹介・CTA)
`pages/pricing.php`	料金プラン比較ページ
`pages/docs.php`	技術ドキュメント・API リファレンス・コード例
`pages/quickstart.php`	5 ステップ統合ガイド (クイックスタート)
`pages/faq.php`	よくある質問
`pages/color-customize.php`	Widget カラーテーマカスタマイズガイド

12. セキュリティ対策

対策	実装
HMAC タイミングセーフ比較	hash_equals() による定時間比較（タイミング攻撃防止）
JWT 有効期限チェック	exp クレームの検証を省略禁止。期限切れ JWT は即座に拒否
Origin 検証	registered domains のみ許可。CORS ヘッダー設定
CSRF 保護	セッションベース API（マイページ）にはトークン検証必須
パスワードハッシュ	PASSWORD_DEFAULT（bcrypt）で保存
Stripe Webhook 署名	HMAC-SHA256 でペイロード署名検証。±5 分のタイムスタンプ許容
SQL インジェクション防止	全クエリ PDO プリペアドステートメント
XSS 防止	全出力 htmlspecialchars() エスケープ