API設計書

ECサイト（汎用オンラインショッピングサービス）

API Design Document - RESTful API

項目	内容
ドキュメントID	EC-DES-003
バージョン	1.0
作成日	2026年2月
作成者	Wai Wai
ベースURL	https://api.your-domain.com
APIバージョン	v1 （例：/api/v1/products）
認証方式	JWT Bearer Token (HttpOnly Cookie)
フォーマット	JSON (Content-Type: application/json)

1. API設計概要

1.1 共通仕様

項目	仕様
ベースURL	https://api.your-domain.com/api/v1
プロトコル	HTTPS（HTTP不可）
認証方式	JWT。ログイン後にHttpOnly Cookieとして保存。 Authorizationヘッダー不要（Cookie自動送信）
レート制限	100リクエスト/分/IP（将来実装）
日時フォーマット	ISO 8601 例：2026-02-18T09:00:00+09:00
文字コード	UTF-8
エラーレスポンス	{ "statusCode": 404, "message": "Not Found", "error": "Not Found" }

1.2 HTTPステータスコード

コード	意味	使用場面
200 OK	成功	GET・PUT・PATCH の正常応答
201 Created	作成成功	POST で新規リソース作成成功
204 No Content	成功（ボディなし）	DELETE 成功時
400 Bad Request	リクエスト不正	バリデーションエラー
401 Unauthorized	認証エラー	JWTなし・期限切れ
403 Forbidden	権限エラー	ロール不足（例：管理者APIへの一般ユーザーアクセス）
404 Not Found	リソースなし	指定IDのリソースが存在しない
409 Conflict	競合	メールアドレス重複など
500 Internal Server Error	サーバーエラー	予期しないエラー

1.3 認証フロー

1. POST /auth/login でJWTアクセストークン（有効期限1時間）とリフレッシュトークン（7日）を発行
2. 両トークンをHttpOnly Cookieに保存（JavaScriptからアクセス不可）
3. アクセストークン期限切れ時：POST /auth/refresh で自動更新
4. 認証が必要なエンドポイントは ☒ で示す

1.4 エンドポイント一覧

グループ	エンドポイント数	概要
認証 /auth	4	ログイン・ログアウト・登録・トークン更新
商品 /products	5	商品一覧・詳細・検索・登録・更新・削除（管理者）
カテゴリ /categories	2	カテゴリ一覧・詳細
カート /cart	4	カート取得・追加・更新・削除

注文 /orders	5	注文一覧・詳細・作成・更新（管理者）
ユーザー /users	3	プロフィール取得・更新・削除
決済 /payments	2	Stripe PaymentIntent作成・確認
管理者 /admin	3	管理者向け集計・ユーザー一覧

2. 認証 API /api/v1/auth

POST	/api/v1/auth/register	☒ 認証不要
概要	新規ユーザー登録。登録後に自動ログイン（JWTをCookieに保存）	
リクエスト ボディ	{ "name": "■■ ■■", "email": "user@example.com", "password": "Password123", "phone": "090-1234-5678", "address": "■■■■■■■..." }	
レスポンス	201: { "id": 1, "name": "■■ ■■", "email": "user@example.com", "role": "USER", "createdAt": "2026-02-18T09:00:00+09:00" } 409: ■■■■■■■■■■ 400: ■■■■■■■■■■■	

POST	/api/v1/auth/login	☒ 認証不要
概要	メールアドレスとパスワードでログイン。JWTをHttpOnly Cookieに保存	
リクエスト ボディ	{ "email": "user@example.com", "password": "Password123" }	
レスポンス	200: { "id": 1, "name": "■■ ■■", "email": "user@example.com", "role": "USER" } 401: ■■■■■■■■■■■■■■■■■■■■■	

POST	/api/v1/auth/logout	☒ JWT必須
概要	ログアウト。Cookie（アクセストークン・リフレッシュトークン）を削除	
レスポンス	200: { "message": "■■■■■■■■■■" }	

POST	/api/v1/auth/refresh	☒ 認証不要
概要	リフレッシュトークンを使用してアクセストークンを更新	
レスポンス	200: ■■■■■■■■■■■■Cookie■■■ 401: ■■■■■■■■■■■■■■■■■	

3. 商品 API /api/v1/products

GET	/api/v1/products	☒ 認証不要
概要	商品一覧取得。カテゴリ・価格・キーワードでフィルタリング、ページネーション対応	
パラメータ	category: string■■■■ ■■electronics sort: price_asc | price_desc | newest■■■■■■■■newest■ page: number■■■■■■■■1■ limit: number■■■■■■■■12■ keyword: string■■■■	
レスポンス	200: { "data": [{ "id": 1, "name": "■■■■", "price": 12800, "stock": 5, "imageUrl": "https://cdn.../img.jpg", "category": { "id": 1, "name": "■■" } }], "meta": { "total": 128, "page": 1, "limit": 12, "totalPages": 11 } }	

GET	/api/v1/products/:id	☒ 認証不要
概要	商品詳細取得。画像・カテゴリ・レビュー情報を含む	
パラメータ	:id → ■■ID■number■	
レスポンス	200: { "id": 1, "name": "■■■■", "description": "■■■■", "price": 12800, "stock": 5, "images": ["url1","url2"], "category": {...}, "reviews": [...], "avgRating": 4.2 } 404: ■■■■■■■■■	

POST	/api/v1/products	☒ JWT必須 + ADMIN
概要	商品新規登録（管理者のみ）	
リクエスト ボディ	{ "name": "■■■■", "description": "■■■", "price": 12800, "stock": 50, "categoryId": 1, "images": ["s3-key1","s3-key2"] }	
レスポンス	201: ■■■■■■■■■■■■■ 400: ■■■■■■■■■■■ 403: ■■■■■■■■	

PATCH	/api/v1/products/:id	☒ JWT必須 + ADMIN
概要	商品情報更新（管理者のみ）。変更するフィールドのみ送信可	
パラメータ	:id → ■■ID■number■	
リクエスト ボディ	{ "price": 9800, "stock": 30 } ← ■■■■■■■■■■■OK	
レスポンス	200: ■■■■■■■■■■■■■ 404: ■■■■■■■■■ 403: ■■■■■■■■	

DELETE	/api/v1/products/:id	☒ JWT必須 + ADMIN
概要	商品削除（論理削除。deleted_atに日時を記録）（管理者のみ）	
パラメータ	:id → ■■ID■number■	
レスポンス	204: No Content 404: ■■■■■■■■■ 403: ■■■■■■■■	

4. カート API /api/v1/cart

GET	/api/v1/cart	☒ JWT必須
概要	ログイン中のユーザーのカート内容を取得	
レスポンス	200: { "items": [{ "id": 1, "product": {...}, "quantity": 2, "subtotal": 25600 }], "totalAmount": 25600, "itemCount": 2 }	

POST	/api/v1/cart	☒ JWT必須
概要	商品をカートに追加。既に存在する場合は数量を加算	
リクエスト ボディ	{ "productId": 1, "quantity": 2 }	
レスポンス	201: ■■■■■■■■■■■■■■ 400: ■■■■■ 404: ■■■■■■■■■	

PATCH	/api/v1/cart/:itemId	☒ JWT必須
概要	カート内の特定商品の数量を変更	
パラメータ	:itemId → ■■■■■■■■ID■number■	
リクエスト ボディ	{ "quantity": 3 }	
レスポンス	200: ■■■■■■■■■■■■ 400: ■■■■■ 404: ■■■■■■■■■■■■■■■	

DELETE	/api/v1/cart/:itemId	☒ JWT必須
概要	カートから特定商品を削除	
パラメータ	:itemId → ■■■■■■■■ID■number■	
レスポンス	204: No Content 404: ■■■■■■■■■■■■■■■	

5. 注文 API /api/v1/orders

GET	/api/v1/orders	☒ JWT必須
概要	ログイン中のユーザーの注文履歴一覧を取得	
パラメータ	page: number limit: number status: string■■■■■	
レスポンス	200: { "data": [{ "id": 1, "orderNumber": "ORD-2026-00123", "totalAmount": 43120, "status": "PROCESSING", "createdAt": "...", "items": [...] }], "meta": { "total": 3, "page": 1 } }	

GET	/api/v1/orders/:id	☒ JWT必須
概要	注文詳細取得。注文商品・配送先・ステータス履歴を含む	
パラメータ	:id → ■■ID■number■	
レスポンス	200: ■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■ 403: ■■■■■■■■■■■■■■■■ 404: ■■■■■■■■■	

POST	/api/v1/orders	☒ JWT必須
概要	カートから注文を作成。Stripe PaymentIntentのconfirm後に呼び出す	
リクエスト ボディ	{ "shippingAddressId": 1, "paymentIntentId": "pi_xxx" }	

レスポンス	201: { "id": 1, "orderNumber": "ORD-2026-00123", "totalAmount": 43120, "status": "PROCESSING" } 400: ■■■■■ / ■■■■ 402: ■■■■

PATCH	/api/v1/orders/:id/status	☒ JWT必須 + ADMIN
概要	注文ステータス更新（管理者のみ）	
パラメータ	:id → ■■ID■number■	
リクエスト ボディ	{ "status": "SHIPPED" } ← PROCESSING|SHIPPED|DELIVERED|CANCELLED	
レスポンス	200: ■■■■■■■■■■■■ 404: ■■■■■■■■	

6. 決済 API /api/v1/payments

POST	/api/v1/payments/create-intent	☒ JWT必須
概要	Stripe PaymentIntentを作成。フロントエンドでStripe.jsを使い決済処理する	
リクエスト ボディ	{ "cartId": 1 } ← ■■■■■■■■■■PaymentIntent■■■	
レスポンス	201: { "clientSecret": "pi_xxx_secret_xxx" } → ■■■■■■■■clientSecret■Stripe.js■■■■■■	

POST	/api/v1/payments/webhook	☒ 認証不要
概要	Stripe Webhookエンドポイント。payment_intent.succeededイベントを受信し注文を確定	
リクエスト ボディ	Stripe■■■■■■■■stripe-signature ■■■■■■	
レスポンス	200: { "received": true } 400: ■■■■■■■	

7. ユーザー API /api/v1/users

GET	/api/v1/users/me	☒ JWT必須
概要	ログイン中のユーザー情報を取得	
レスポンス	200: { "id": 1, "name": "■■ ■■", "email": "...", "phone": "...", "addresses": [...], "role": "USER" }	

PATCH	/api/v1/users/me	☒ JWT必須
概要	ユーザー情報更新（氏名・電話番号・住所）	
リクエスト ボディ	{ "name": "■■ ■■", "phone": "090-9999-9999" }	
レスポンス	200: ■■■■■■■■■■■■■■■ 400: ■■■■■■■■■■■	

GET	/api/v1/users	☒ JWT必須 + ADMIN
概要	ユーザー一覧取得（管理者のみ）	
パラメータ	page: number limit: number keyword: string■■■■	
レスポンス	200: { "data": [{...}], "meta": { "total": 1024 } }	

8. 画像アップロード /api/v1/uploads

POST	/api/v1/uploads/presigned-url	☒ JWT必須 + ADMIN
概要	S3へ直接アップロードするためのPresigned URLを発行（管理者のみ）	
リクエスト ボディ	{ "filename": "product-image.jpg", "contentType": "image/jpeg" }	
レスポンス	201: { "uploadUrl": "https://s3.amazonaws.com/...", "key": "products/uuid-filename.jpg", "cdnUrl": "https://cdn.your-domain.com/products/uuid-filename.jpg" } → ■■■■■uploadUrl■■■■PUT request■■■■■■S3■■■■■■■	

9. エラーレスポンス例

9.1 バリデーションエラー（400）

```
{ "statusCode": 400, "message": ["email must be an email", "password must be longer than 8 characters"], "error": "Bad Request" }
```

9.2 認証エラー（401）

```
{ "statusCode": 401, "message": "Unauthorized", "error": "Unauthorized" }
```

9.3 権限エラー（403）

```
{ "statusCode": 403, "message": "Forbidden resource", "error": "Forbidden" }
```

10. 改訂履歴

バージョン	日付	変更者	変更内容
1.0	2026/02	Wai Wai	初版作成