CMS/EC パッケージ

はじめに

CMS/ECパッケージは、広く普及しているウェブアプリやサービスをAPIで連携させ、個々のスタイルに合わせてカスタマイズし、まるでテイラーメードされたかのようなホームページとECサービスをスピーディーかつリーズナブルに構築するように設計されたパッケージです。
また、普段は気にはしつつも見落としがちなネットワークセキュリティに関して、スペシャリストの目から見てセキュアな状態を保つように設計されています。
もちろん、クレジットカード決済に関する部分は最新のPCI-DSS（現在はv.3.1.2）に完全準拠するように設計しています。セキュアなシステム環境を維持できることは、特に決済を伴うECサイトでは不可欠な選定要素です。

基本設計

設計思想として以下のような要件を満たすためにデザインされています。

基本項目の表示速度

UXのみならず、SEO対策としても重要

内部・外部への拡張性と柔軟性

外部システムとのAPIによる連携
- プラグインにより連携サービスを拡張可能
- データの不保持化と分散化につながる

フロンエンドへのAPI提供
- フロントエンドとバックエンドの分割が可能
- フロントエンドのコーディングの自由度が増加

WebSocketの融合

チャットシステムなどで不可欠な要素

情報の不保持化

決済ベンダー等が提供するセキュアなシステムがキーデータを保存
必要最低限の情報のみを保持することで、万が一の場合のデータ漏えいによる被害を最小限に食い止めます

ネットワークセキュリティ対策

ポピュラーなオープンソースソフトウェアやフレームワークを使わずに構造を秘匿化
独自の侵入防止対策を標準で実装
その他基本的なセキュリティ対策を徹底

これらの要件を満たすフレームワークとして、CMS/ECパッケージではTornadeを標準のフレームワークとして選択します。
TornadoはWebSocketをサポートし、非常に高速で動作するPythonフレームワークとして知られています。また、必要とされる要件に応じて、動作速度はやや落ちますが、オプションで日本国内でもポピュラーなdjangoをフレームワークとして選択していただくことも可能です。

Tornado / Django の特徴比較（弊社見解に基づく）

	動作速度	メンテナンス性	カスタマイズ性	WebSocket	開発者数
Tornado	★★★★★	★★★★☆	★★★★★	★★★★★	★☆☆☆☆
Django	★★☆☆☆	★★★★★	★★★★☆	★★★☆☆	★★★★★

機能補足

設計思想として以下のような要件を満たすためにデザインされています。

IT補助金既定のITツール

①決済機能（電子決済機能をStripe等との連携により実装）
②EC機能（WEBサイト上で商品を販売する電子商取引の機能）

インボイス対応

・発注者側が受注者側の適格請求書発行事業者登録番号（インボイス管理番号）を管理する機能を有しない
・インボイス制度に対応した受発注機能を有しない

実装される機能と拡張機能

EC基本パッケージ

CMS	
コンテンツ一覧・選択表示	◎
コンテンツ詳細表示	◎
AI全文検索	◎
固定ページ作成・管理	◎
ブログ・ニュース投稿・管理	◎
LP・キャンペーン投稿・管理	◎
商品情報作成・管理	―
予約投稿・削除	◎
規約等の作成・管理	◎
チャットQ&A	
リアルタイム応答	◎
検索AI応答bot	◎
生成AI応答bot	○
Eコマース	
ショッピングカート	◎
クレジットカード決済	◎
受発注管理	◎
顧客管理	◎
税率・配送料等の設定	◎
クーポン発行	○
ポイントカード発行	○
チャット受発注	○
会計ソフトウェア連携	※1
銀行口座連携	※2
その他	
独自ドメイン	◎
常時SSL化（HTTPS）	◎
レスポンシブ対応	◎
基本的なSEO対策	◎
位置情報との連携	○
各種SNS連携	※3
OAuth2による認証	※4

コーポレートサイト	
会社概要	○
お知らせ一覧	○
お知らせ詳細	○
お問い合わせフォーム	○
ECサイト	
ブランド一覧	◎
ブランドトップ	◎
商品一覧	◎
商品詳細	◎
ショッピングカート	◎
お知らせ一覧	◎
お知らせ詳細	◎
お問い合わせフォーム	◎
ブログ	
ブログトップ	
ブログ記事一覧	◎
ブログ記事	◎
各種ガイド・規約等	
ご利用規約	◎
ご利用ガイド	◎
特定商取引法に関する表示	※5
プライバシーポリシー	◎
顧客用ダッシュボード	
認証ページ	◎
個人情報	◎
購入履歴	◎
管理者用ダッシュボード	
認証ページ	◎
ユーザー管理	◎
販売管理	◎
固定ページ管理	◎
ブログ記事管理	◎

◎ 標準装備　○ 拡張オプション　― 設定なし

※1 Freeeでの実装となりますが、APIの取得が可能な他会計ソフトウェアでも対応が可能です（別途お見積もり）
※2 2023年9月時点ではAPIの公開範囲の制約から、GMOあおぞらネット銀行の法人口座のみの対応となります
※3 Facebook・Instagram・X（旧Twitter）以外の対応は別途お見積もりとなります
※4 Google・Facebook・Instagram・X（旧Twitter）以外の対応は別途お見積もりとなります
※5 取扱商品が表示義務に該当する場合はパッケージに含まれます

フレームワークとAPI可能連携アプリ

Tornado	サーバーと一体化したフルスタックWebフレームワークでシステムの基幹部分
Algolia	AIによる検索エンジンで、パッケージ内では全文検索システムを構築
ChatGPT	生成AIエンジンとしてパッケージ内では商品情報などをインタラクティブに表示
Google Photo	システム内の画像ファイルを管理
Stripe	ECシステム内で決済機能を実装（PAY.JPへの変更もパッケージ内で可）
Freee	ECシステムの取引を会計システムと連携させて記帳

基本的なセキュリティ対策

予防的対策	
各種認証画面のステルス化	ブラウザ以外からのアクセスでは空白のページが表示されます
常時HTTPS接続	通信を秘匿化することで通信の安全性を引き上げます
XSS対策	クロスサイトスクリプティング対策を実施して脆弱性を減らします
インジェクション攻撃対策	インジェクション攻撃対策を実施して脆弱性を減らします
ブルートフォース攻撃対策	ブルートフォース攻撃対策を実施して脆弱性を減らします
事後的対策	
ディレクトリ構造の秘匿	侵入された場合でも目的のファイルの所在を明かさないことで時間を稼ぎます
管理者権限の保護対策	侵入された場合でもすぐに管理者権限を取られないようにして時間を稼ぎます
情報の不保持化	攻撃を実行されたとしても情報の不保持化で情報漏洩を防ぎます
情報の分散化	情報が漏洩した場合でも情報を細分化することで無意味化して被害を低減します
情報のトークン化	情報が漏洩した場合でもハッシュ暗号化（トークン化）することで被害を低減します

情報収集

◎各種認証画面のステルス化
◎常時HTTPS接続
サーバ監視

侵入の試み

◎XSS対策
◎インジェクション攻撃対策
◎プルートフォース攻撃対策
サーバ監視

侵入成功

◎ディレクトリ構造の秘匿
◎管理者権限の保護対策
サーバ監視

サーバ操作

◎情報の不保持化
◎情報の分散化
◎情報のトークン化
サーバ監視

被害額算出
（フォレンジック）

価格(税抜き)

５５０万円