AI.SHOKU / PEOPLE MEET OPPORTUNITY

サービス・導入マニュアル

日本語 / ネイティブPHP・MySQL / 承認済みデザイン版

Version 1.1.0-rc1 • 22 September 2026

> 自社Linuxサーバー、MySQLデータベース、HTTPSドメイン向け。

目次

01 実行環境とリリース範囲

02 Linuxサーバーへの導入

03 ドメイン、HTTPS、ポータルセッション

04 AI、メール、任意の音声機能

05 ワーカー、保守、安全な操作

06 データ、保持、バックアップ、更新

07 実候補者の処理前の受入確認

ローカル検証と本番受入は異なります。実候補者データを処理する前に、リリース承認記録を確認してください。

実行環境とリリース範囲

対象環境はPHP 8.3以降、PHP-FPM、PDO MySQL、MySQL 8.4です。Linuxにsodium、openssl、fileinfo、curl、mbstring、DOM/XML、ZIP、iconv、および書類処理用のpdftotext、GNU timeout、ClamAVが必要です。実行時のサードパーティComposerパッケージやPython/Nodeバックエンドは不要です。

承認済みのデザインはPHP APIとサーバー側の権限制御に接続されています。公開済み根拠、応募、面接、通知、監査情報は、移行管理を含む32のMySQLテーブルに保存されます。スキーマの移行番号は001のままです。

コードとローカルテスト記録を提供するものであり、本番認証ではありません。対象MySQL、HTTPS上のネイティブ多要素認証、SMTP、AI、音声、スキャン、負荷、復旧、アクセシビリティは貴社環境での受入確認が必要です。パッケージ作成により稼働中サーバーやドメインが変更されることはありません。

Linuxサーバーへの導入

1. コマンド実行前にdocs/SETUP_LINUX_EN.mdまたはSETUP_LINUX_JA.mdを確認してください。Ubuntu用補助スクリプトは24.04/PHP 8.3を対象とし、既存のMySQLサーバーを置き換えません。
2. コードは公開ディレクトリ外に配置し、ドキュメントルートを/var/www/aishoku/publicに設定します。Web実行アカウントにはコードを書き込ませず、非公開ストレージは/var/lib/aishokuに保存します。chmod 777は使用しないでください。
3. HTTPSオリジンを指定してsetupを実行し、一度だけ.envを作成します。APP_KEYを紛失・変更すると暗号化データを読めなくなるため保持してください。秘密情報はソース管理やチャットではなく、安全な場所に保存します。
4. DB管理者が専用UTF-8データベースと実行用・移行用の別アカウントを作成します。初回移行は空のDBに一度だけ実行します。移行エラーの解消のために顧客DBを初期化しないでください。

```
cd /var/www/aishoku
sudo php bin/console setup --url=https://jobs.example.com --environment=production
# Edit .env privately; replace the placeholder domain.
sudo php bin/console migrate --credentials-file=/etc/aishoku/migration.env
sudo -u www-data php bin/console preflight
```

> 上記ドメインは例示であり、公開済みのAi.shokuアドレスではありません。所有者、権限、移行アカウントファイルの設定は完全な導入ガイドに従ってください。

ドメイン、HTTPS、ポータルセッション

1. DNSレコードを対象ホストに向けます。証明書を発行した後、正しいPHPソケットと証明書パスを設定したNginxまたはApache/FPMテンプレートを有効にします。他のサイトは変更しないでください。
2. 実行可能なWebエントリーポイントをpublic/index.phpだけに限定し、.env、app、database、tests、storageへの公開アクセスを禁止します。
3. APP_URLおよび必要に応じて4つのポータルURLを設定します。個別URLにはポータルパスを含めます。Secure、HttpOnly、SameSite Cookieとサーバーセッションは用途ごとに分離されますが、同一ドメイン上のパスは別のブラウザーオリジンではありません。
4. 実際のHTTPSオリジンに対してdeploy/verify-domain.shを実行し、デスクトップとiPhone/Androidブラウザーでログインおよび操作を確認します。このチェックは公開や変更を行いません。

```
sudo nginx -t
sudo systemctl reload nginx
sudo systemctl reload php8.3-fpm
bash deploy/verify-domain.sh https://YOUR-REAL-DOMAIN
```

> 読み込みが終わらない旧プレビューに代えて、サーバーが読めるHTML、マニュアルリンク、時間制限付きの復旧メッセージを表示します。ただし、未配備のファイルをライブアプリケーションにする機能ではありません。

AI、メール、任意の音声機能

設定項目	必要な設定
AI	AI_MODE=live; AI_BASE_URL; AI_MODEL; AI_API_KEY; AI_DAILY_CALL_LIMIT
Mail	MAIL_TRANSPORT=smtp; MAIL_FROM; SMTP_HOST; SMTP_PORT; SMTP_ENCRYPTION; SMTP_USERNAME; SMTP_PASSWORD
Help	AI_HELP_ENABLED=true only after provider approval; default false
Voice	VOICE_ENABLED=true; STT_MODEL; TTS_MODEL; TTS_VOICE
Notice	PRIVACY_CONTACT; AI_PROVIDER_DISCLOSURE; DATA_REGION_DISCLOSURE

AI_BASE_URLは付属のJSONチャットおよび任意の音声契約を実装する必要があります。互換性の表示だけで動作が保証されるわけではありません。JD、履歴書、回答は信頼されない入力として扱います。出力はスキーマ、ID、引用検証を通過する必要があり、スコア計算と権限は決定的なコードが制御します。人による確認は引き続き必要です。

メールサービスでSPF、DKIM、DMARCを設定します。ステージングでは宛先許可リストを指定してください。SMTP受理は受信箱への到達証明ではありません。バウンス・苦情の取り込みは配信サービスごとに追加連携が必要です。

PSTN電話発信、全二重音声エージェント、動的な面接追加質問、外部カレンダー同期、SAML/OIDC/SCIM、請求、ATS連携は完成済みモジュールとして含まれません。

ワーカー、保守、安全な操作

付属のsystemdワーカーと毎分スケジューラーを有効にします。両者は同じ非公開設定、固定の暗号鍵、DB、永続ストレージを利用します。起動後に状態とログを確認してください。管理画面が示すのはタスク状態と論理的なメール状態であり、外部サービスの配信保証ではありません。

```
sudo systemctl enable --now aishoku-worker.service
sudo systemctl enable --now aishoku-scheduler.timer
sudo systemctl status aishoku-worker.service
sudo journalctl -u aishoku-worker.service -n 100
```

タスクには重複防止キー、リース、回数制限付きの再試行、失敗確定状態があります。再試行前にエラーコードを確認してください。外部処理が常に厳密に一度だけ実行される保証はありません。SMTP結果が不明な場合は照合してから再送します。

古いキュー、失敗・不確定メール、ディスク、DB、プロセス、証明書期限、API遅延、クォータを監視します。/healthzはエントリーポイント、/readyzはDB接続を確認しますが、全依存サービスを検証するものではありません。外部アラート基盤は同梱されません。

データ、保持、バックアップ、更新

承認済み求人・プロフィールの版、回答、レビュー、一部の監査・根拠レコードは変更不可です。テナント権限はPHPのポリシークエリで制御し、MySQLの行レベルセキュリティ機能を実装したとは主張しません。個人テキストと原本はアプリ鍵で暗号化しますが、すべてのメタデータや識別子が暗号化されるわけではありません。

承認済み方針のもとで--applyを付ける前に、documents:purgeで原本の保持期限処理をプレビューしてください。公開プロフィールや面接の全情報を削除する処理ではありません。削除依頼は処理を停止し、権限を持つ担当者の確認を必要とします。

DB、暗号化された非公開ファイル、APP_KEYを、整合性のある復旧可能な組としてバックアップします。鍵を無制限に閲覧できる同一アーカイブに格納しないでください。送信通信を遮断した隔離ホストで復旧を試験し、トリガー、定義者、権限、復号、キューを再確認します。RPO/RTOは推測せず測定して記録します。

> PHP 1.0.0-rc1から更新する場合は既存の.env、APP_KEY、ストレージを保持します。1.1.0-rc1に新しいスキーマ移行はありません。受入試験を再実行してワーカーを再起動します。旧Python/PostgreSQL版や既存SESサイトからの自動移行ではありません。

実候補者の処理前の受入確認

1. 破棄可能な*_test MySQL DBで試験し、実際のDBバージョンで移行、トリガー、DML専用アカウント、ユニーク制約、予約・ワーカーの並行実行を確認します。
2. 実ドメインでHTTPS、ブラウザーセッション、ポータル境界、MFA、CSRF、メール確認・再設定、アカウント失効を試験します。
3. 英語・日本語で架空データによる採用フローを完走し、メール到達、タイムゾーン、実マイク操作、人によるレビューを確認します。
4. 日本語・英語の代表的な履歴書・求人で、人が評価したデータセットによるマッチング・採点を検証します。根拠不足や保護属性への感度も確認します。計算の単体試験だけではモデル品質を示せません。
5. 脆弱性・依存関係レビュー、ファイル隔離・スキャン、プライバシー・法務確認、アクセシビリティ・モバイルUAT、負荷試験、復旧訓練を実施します。承認者を指名し、証跡を添付してください。

docs/PRODUCTION_GATES.mdとdocs/TEST_RESULTS.mdをリリース記録として利用してください。この単一ホスト構成は高可用性や無制限の企業規模への対応を保証しません。