賀恋棚 (が れんほう)



Java バックエンド / Agent アプリケーション開発
2026 年卒。Java を軸に Python/LangGraph Agent を業務 API と連携し、認証の隔離、出典の境界、明示的確認後の保存を実装。
重慶
採用担当の方は、関心をお持ちいただけましたらメールでご連絡ください。·メール· lysf15520112973@163.com ·GitHub ·DavidHLP ·知識庫

主な強み

- **Java API と Agent**：既存 Java の認証・データ認可を維持し、Python/FastAPI・LangGraph で制御されたツール呼び出し、出典付き分析、複数ターン会話を実装。
- **復元可能な操作**：owner 検査、草稿バージョン、明示的確認、同一冪等キーでの照合により、取消・古い確認・書込結果不明に対応。実装と正式受入検証は区別。
- **境界の検証**：一般ユーザー 2 アカウントの HTTP 対照、実モデルへの攻撃入力、引用検査で隔離を確認。なりすまし、他アカウントへの要求、出典への指示注入を検証。

実習経験

博彦科技（Beyondsoft）
2026.01 - 2026.06
バックエンド開発インターン｜ Alibaba Cloud 専有クラウド・Aegis ホストセキュリティ

- **リソース連携**：Alibaba Cloud 専有クラウドの Aegis セキュリティ製品のバックエンド開発に参加。プラットフォーム/ECS/BMS/BMCP と連携し、GPU 情報の取り込み・集約を独力で実装して統計・絞り込み・関連検索を支援。
- **AI 資産識別**：機能開発に参加し、OpenClaw/Ollama のテスト用コンテナーを独力で構築。コンテナー状態、GPU 関連、脆弱性データから資産状態・関連付け・リスク表示を実装。
- **検索最適化と障害修正**：SQL 実行計画、インデックス、条件、対象フィールドを調整し、一覧/統計検索の時間を短縮。Arthas `watch` / `trace` / `stack` で経路・時間・例外・引数を調べ、不具合修正と回帰検証を独力で実施。
- **イメージ信頼チェーン調査**：containerd による Harbor プライベートイメージ取得時の TLS 障害を特定。CA、`certs.d`、`hosts.toml`、`imagePullSecrets`、ノードキャッシュを調べ、診断スクリプトとチェックリストを整備。

プロジェクト経験

オンラインプログラミング評価システム UltiCode GitHub
Java 17 / Spring Boot 4 / Spring Security / MySQL / Redis Streams / Dubbo / Flyway / Docker
個人開発の OSS 評価システム。Java サービスが認証・問題・提出・業務記録を保持し、独立した Judge Worker が判定を実行。Agent は既存 HTTP 契約から業務に接続する。

- **信頼性の高い配信**：提出と Outbox を同一トランザクションで記録し、Redis Streams へバックオフ再試行付きで配信。Lua で重複排除マーカーとキュー追加をまとめ、タイムアウト回収とデッドレターで障害区間に対応。
- **実行結果の競合制御**：`generation` + `attemptId`、リース、ハートビートで有効な実行を識別。SQL CAS が古い判定を拒否し、Docker が信頼できないコードの権限と資源を制限。
- **認証と検証**：リフレッシュトークンをハッシュで保存し、一度限りの消費とトランザクション内の更新に対応。実 MySQL 移行、ブラウザー・Judge のログイン、AC/WA、再判定、順位表を CI で検証。

UltiCode Agent 業務連携（実験機能）ソース
Python / FastAPI / httpx / LangGraph / SQLite / SSE / MCP / Java Auth & App API
本人の通常練習提出を対象に、制御された分析、複数ターンの会話、任意の学習計画を提供。認証と業務データの権限は Java が保持し、Agent は私有会話とローカルワークフロー状態を管理する。

- **信頼できる認証とツール境界**：Java `/auth/me` で本人を確認し、リクエストごとに Cookie クライアントを分離。許可リスト内の読み取り専用ツールだけを公開し、引数と返却フィールドを検査・投影。モデルによる所有者の指定や書き換えを許可しない。
- **有界のモデル・ツールループ**：LangGraph でモデル、ツール、結果を編成し、ラウンド数と総時間を制限。ツール失敗、上限超過、キャンセルを区別し、ツール結果をデータとして扱って越権命令には従わない。
- **会話とチェックポイント**：SQLite で owner、conversation/turn、thread/run、草稿バージョンを管理。復元時に所有権を再検査し、キャンセルのフェンスで古い実行の保存を防ぐ。会話履歴と学習計画スレッドは分離。
- **明示確認と結果照合**：編集後は古い確認を無効化し、保存前に現行バージョンとダイジェストへ結び付けた確認を別途要求。Java の書き込み結果が不明なら未確定状態を保ち、同じ冪等キーで読み戻す。新しいキーで盲目的に再試行しない。
- **資料と MCP 投影**：出典の範囲・バージョン・位置を保持。許可済みソースコードはリクエスト内だけで利用し、会話・イベント・チェックポイントへ保存しない。任意の stdio MCP は認証済みクライアントと厳密な投影を再利用し、本人の提出一覧だけを公開。

2 アカウントの HTTP/モデル隔離と出典付き分析の段階検証記録を確認。学習計画の書込・障害復旧の正式受入完了は主張しない。ライブ分析と永続化は個別に明示的に有効化し、本番配備・実ユーザー試行は主張しない。

専門スキル

Java バックエンドと信頼性

- Java、Spring Boot、Spring Security、MyBatis-Plus に習熟。API 設計、認証・認可、MySQL 最適化、トランザクション境界の実践経験。
- Redis のキャッシュ保護、分散ロック、Streams、Outbox、Docker 隔離の実装経験。再試行、重複消費、結果整合性を理解。
- Arthas、SQL 実行計画、Linux、コンテナーログで調査し、並行テスト、Testcontainers、CI で障害条件を検証。

Agent アプリケーションと業務連携

- Python、FastAPI、httpx、LangGraph の実装経験。既存 Java API を使い、ツール呼び出し、タイムアウト、キャンセル、ストリームイベントを構成。
- サーバー認証、許可ツール、フィールド投影、資料の同意とコンテキスト境界を実践。モデルの提案、利用者の確認、業務書き込みを区別。
- SQLite の会話・チェックポイント、所有権・バージョン検査、冪等保存、不明な結果の照合を実践。制御されたテスト、実サービス検証、本番提供を区別。

学歴・受賞

学歴

洛陽師範学院

データ科学とビッグデータ技術・学士課程

GPA: 3.6 / 4.0 (2021.09 - 2026.07)

受賞

- 2025 藍橋杯 Java ソフトウェア設計 B 組・**全国三等賞**
- 2024 テディ杯データ分析技能競技・**全国三等賞**
- 2023 全国大学コンピューター能力挑戦・**全国三等賞**

OSS 貢献と技術記録

OSS 貢献

codebase-memory-mcp：Oh My Pi クライアント接続、MCP 登録、インストール・アンインストールと利用者設定の保護に貢献。Linux の信頼できるシステムパスとの互換性を修正し、回帰テストを追加。

代表的な技術知識頁

- Java 性能障害：現象から証拠への最小判断木：プロセス、スレッドスタック、GC、Arthas の観測をつなぎ、影響の抑制・証拠保全・問題特定・復旧の手順を整理。
- UltiCode Outbox と Redis Streams：判定タスクの配送を復旧可能な状態にする：トランザクション Outbox、原子的な配送、再試行、デッドレターと未確認メッセージの回収を整理。