Statement of Work SOW

NexSupply AI Driven Factory Verification Platform

버전 1.3 Final

작성일 2026년 2월 3일

프로젝트 리드 Myungjun Kim CEO

목표

구축 비용을 최적화하면서 글로벌 공급망 데이터의 신뢰성을 확보하는 AI와 인간 검증 HITL 결합형 플랫폼 구축

0 핵심 원칙 한 줄

이 플랫폼은 Claim 기반 데이터 불변성과 Evidence 기반 검증, Slack 중심 운영, Resolved View 스냅샷으로 빠른 초기 운영과 장기 확장을 동시에 확보한다

1 프로젝트 범위와 결과물

1.1 포함 범위

- 유저 입력
- 제품 사진 또는 제품명으로 분석 요청
- Phase 1 Free Analyze
- 무료 가설 H 리포트 생성
- Blueprint 결제 유도
- Phase 2 Blueprint 49
- 결제 승인 후 공장 후보 매칭
- 데이터 수집과 문서 요청
- Phase 3 Final Verification
- 증거 서류 업로드
- AI 추출
- Auditor 검증과 승인
- 최종 확정 V 리포트 발행
- Slack 기반 운영
- 알림
- 승인
- 반려
- 추가 서류 요청
- 상태 전이 관리
- 감사 추적 Audit Trail
- 데이터 출처

- 변경 이유
- 행위자 기록
- 쿠폰과 크레딧
- 이벤트용 쿠폰 코드 발급
- 크레딧 지급
- 결제 할인 적용
- 보안
- Signed URL 기반 파일 접근
- 짧은 만료
- 권한 없는 접근 차단

1.2 제외 범위

- 대규모 엔터프라이즈 기능
- 다수 조직 복잡 권한
- SSO
- 복잡한 청구 체계
- 완전 자동 공장 검증
- 사람 검증 없이 V Lock 자동 확정은 하지 않는다
- 대규모 크롤링 인프라
- 수만 SKU 동시 수집용은 범위 밖이다

1.3 최종 결과물 Deliverables

- 웹 대시보드 User
- 프로젝트 생성과 리스트
- 상태 표시
- H와 V 리포트 렌더링
- 쿠폰과 크레딧 적용
- 문서 업로드
- Auditor Desk
- 조회 중심
- 문서 뷰어
- Claim 히스토리 조회
- Evidence 링크와 Audit 로그 확인
- Side by Side 검토 화면 권장
- Slack 운영 도구 핵심
- 프로젝트 이벤트 알림
- Confirm Payment
- Verify
- Reject
- Need more docs

- Claim 기반 데이터 모델
- 감사 로그
- 상태 전이 이벤트 시스템
- 결제 로직
- 초기 수동 승인 기반
- 확장 시 Stripe 도입 가능한 구조
- Verified 리포트 PDF 출력
- 템플릿 포함
- Verified by NexSupply 인장 포함

2 기술 스택과 인프라 원칙

2.1 권장 스택

- Identity
- Firebase Auth
- Compute
- Cloud Run Docker
- DB
- Cloud SQL PostgreSQL
- JSONB 적극 활용
- Storage
- Google Cloud Storage
- Signed URL
- AI ML
- Vertex AI Gemini
- Context Caching
- Async
- Cloud Tasks 또는 Pub Sub
- DLQ 포함
- Ops
- Slack API
- OAuth
- Interactivity
- Payment
- 초기 수동 승인
- 추후 Stripe Checkout과 Webhook

2.2 운영 원칙

- 장기 작업은 비동기 처리
- 크롤링

- OCR
- PDF 생성
- 이메일 발송
- 스냅샷 재계산
- 모든 데이터 변경은 이벤트로 기록
- 누가
- 언제
- 무엇을
- 왜
- 파일 접근은 Signed URL로 최소 권한과 짧은 만료
- 기본 10분에서 15분
- Idempotency 필수
- Slack 버튼
- 큐 재시도
- 결제 이벤트
- 중복 처리 금지
- 환경 분리
- dev
- stage
- prod
- 시크릿, 버킷, 웹훅 분리

3 핵심 설계 개념

3.1 Claim 기반 데이터 모델

- 기존 레코드를 수정하지 않는다
- 데이터는 Claim으로 누적한다
- 가장 신뢰 가능한 Claim을 Verified로 잠금하여 보고서와 계산의 기준으로 삼는다
- Verified 이후 수정이 필요하면 기존 Claim을 수정하지 않는다
- 새 Claim 발행
- 새 Verified 버전으로 잠금

3.2 H to V 데이터 구분

- H Hypothesis
- AI 기반 추정
- 참고용
- V Verified
- Evidence와 Auditor 승인 기반 확정

3.3 Resolved View 스냅샷

- 리포트 렌더링 성능과 PDF 재현성을 위해 프로젝트별 현재값을 JSONB 스냅샷으로 유지한다
- 스냅샷은 Claim 조인 결과를 미리 계산한 값이다
- Verified 완료 시점에는 Verified Snapshot을 고정 저장한다
- 재현 가능한 PDF
- 정산 기준 보장

4 사용자 플로우

4.1 Phase 1 Free Analyze

- 입력
- 제품 사진 또는 제품명
- 처리
- 카테고리 추정
- FOB 범위
- Duty
- HS 후보
- 출력
- H 리포트
- Blueprint 언락 유도

4.2 Phase 2 Blueprint 49

- 트리거
- 유저가 Unlock 클릭 후 결제 요청
- 처리
- 공장 후보 3곳 이상 매칭
- 소스 링크 수집
- 프로젝트별 GCS 폴더 생성
- 필요 서류 요청
- 출력
- 후보 리스트
- 비용 모델
- 리스크 표시

4.3 Phase 3 Final Verification

- 처리
- Auditor가 문서와 수출 실적을 대조
- AI 추출값을 Side by Side로 검토
- Verified Claim 확정
- 리포트 잠금
- 출력

- Verified by NexSupply 인장
- PDF 발행
- Execution Fee 계산 가능 상태

5 상태 머신 정의

5.1 상태 목록

최소

- ANALYZING
- WAITING_PAYMENT
- BLUEPRINT_RUNNING
- AUDIT_IN_PROGRESS
- VERIFIED

운영상 권장 확장

- FAILED
- CANCELLED
- REFUNDED
- EXPIRED

5.2 전이 규칙 핵심

- 결제 승인 완료 시에만 BLUEPRINT_RUNNING 진입
- BLUEPRINT_RUNNING 실패 시 AUDIT_IN_PROGRESS로 전환 가능
- 유저 화면에는 전문가 검토 진행 중으로 표시
- Slack 알림 발송
- VERIFIED 전이는 관리자만 가능
- VERIFIED 이후 핵심 값 수정 금지
- 수정 필요 시 새 Claim과 새 Verified 버전만 허용

5.3 중복 방지

- 모든 전이 이벤트는 idempotency key를 가진다
- 큐 작업은 재시도 정책과 DLQ를 가진다

6 데이터 모델 최소 구성

6.1 projects

필수

- project_id
- owner_user_id

- status
- gcs_folder_path
- is_paid_blueprint
- created_at
- updated_at

권장

- resolved_view_jsonb
- resolved_view_updated_at
- verified_snapshot_jsonb
- verified_at
- verified_version_id

6.2 sourcing_claims

필수

- claim_id
- project_id
- field_key
- value_json
- claim_type
- HYPOTHESIS
- USER_PROVIDED
- VERIFIED
- confidence
- created_by
- ai
- user
- auditor
- system
- created_at

권장

- currency
- unit
- source_type
- model
- crawl
- document
- source_ref
- version_id

6.3 evidence_files

필수

- evidence_id
- project_id
- gcs_path
- mime_type
- sha256
- size_bytes
- uploaded_by
- created_at

권장

- original_filename
- virus_scan_status

6.4 claim_evidence_links

- claim_id
- evidence_id
- created_at

6.5 audit_actions

필수

- action_id
- project_id
- actor_id
- action_type
- verify
- reject
- edit_note
- request_more_docs
- status_transition
- confirm_payment
- coupon_redeem
- credit_apply
- note
- created_at

권장

- request_id
- idempotency_key

6.6 project_status_events

필수

- event_id
- project_id
- from_status
- to_status
- actor_id
- reason
- created_at

권장

- idempotency_key
- source
- ui
- slack
- system

6.7 credits_ledger

필수

- ledger_id
- user_id
- project_id nullable
- amount_cents
- reason
- coupon
- campaign
- refund
- adjustment
- rollback
- source_id
- created_at

권장

- balance_after 또는 별도 집계 뷰

6.8 coupons 캠페인

필수

- coupons
- coupon_redemptions
- campaigns

권장

- per_user_limit
- min_payment_cents
- eligible_product
- blueprint
- execution

선택

- workspaces
- workspace_members

7 가격과 계산 로직

7.1 Blueprint Fee

- 49달러 고정

7.2 Execution Fee

- max FOB_Total 곱하기 0.10, 500

7.3 Total Landed Cost

- LandedCost는 다음을 따른다
- FOB 더하기 Freight 더하기 Insurance
- 위 합에 DutyRate를 반영
- 마지막에 1.15 버퍼를 상시 포함

8 쿠폰과 크레딧 설계

8.1 원장 기반 원칙

- 쿠폰 입력 시 credits_ledger에 적립 플러스 기록
- 결제 시 credits_ledger에 사용 마이너스 기록
- 실패나 취소 시 rollback 플러스 기록

8.2 적용 규칙

- Stripe 도입 전에도 동일 규칙을 유지한다
- 결제 금액은 최소 1달러를 유지한다
- 쿠폰은 계정당 1회 또는 캠페인 정책으로 제한한다

9 운영과 어드민 흐름

9.1 Slack 중심 운영 원칙

- 초기에는 Admin UI로 승인하지 않는다
- 승인, 반려, 추가 서류 요청은 Slack 버튼으로 처리한다
- Admin UI는 조회와 감사 추적 확인용이다

9.2 Slack 알림 이벤트

- 신규 프로젝트
- Blueprint 요청
- 서류 업로드
- 상태 전이 실패
- 큐 작업 실패

9.3 Slack Quick Auditor 버튼

- Confirm Payment
- Verify
- Reject
- Need more docs

버튼 클릭 시 필수 처리

- audit_actions 기록
- project_status_events 기록
- Slack 메시지 업데이트
- idempotency 적용

9.4 Auditor Desk 핵심

- 문서 뷰어 Signed URL
- Claim 히스토리와 Evidence 링크
- Verify 시 Verified Snapshot 생성과 고정 저장

10 보안과 신뢰성

10.1 보안

- Cloud Run과 Cloud SQL 사설 통신
- Secret Manager로 키 관리
- Signed URL 만료 필수
- 역할 기반 권한
- user
- auditor
- admin
- system

- 파일 업로드 정책
- 확장자 제한
- 용량 제한
- sha256 무결성 검증
- 악성 파일 스캔 상태 저장 권장

10.2 신뢰성

- 큐 기반 비동기 처리
- 재시도
- DLQ
- Slack 버튼, 큐 작업, 결제 이벤트는 idempotency key 필수
- 실패 시 유저 메시지
- 전문가 검토 진행 중
- 실패 시 Slack 알림

10.3 관측 Observability

- 모든 API 요청에 request_id
- 상태 전이 이벤트 로깅
- AI 호출 토큰, 응답 시간, 비용 기록
- 프로젝트별 예산 상한과 초과 시 degrade 정책 권장

11 결제 워크플로우

11.1 초기 수동 승인 흐름

- 유저가 Unlock Full Blueprint 클릭
- 프로젝트 상태를 WAITING_PAYMENT로 변경
- 유저에게 요청 완료 메시지 노출
- 입금 안내 이메일 발송
- Slack에 결제 요청 알림 발송

11.2 운영자 승인

- 운영자가 입금 확인 후 Slack에서 Confirm Payment 클릭
- 클릭 즉시 is_paid_blueprint true
- status를 BLUEPRINT_RUNNING으로 전환
- 파이프라인 작업 enqueue

11.3 고객 이탈 방지 문구

- 입금 안내와 화면에 평균 15분 내 활성화 기대 문구 포함

12 Definition of Done

12.1 기능

- 사진 업로드 후 프로젝트 생성 가능
- 리포트 화면 렌더링 가능
- Blueprint 요청 가능
- WAITING_PAYMENT 전환과 사용자 안내 노출
- Slack 결제 요청 카드 수신
- Slack Confirm Payment로 파이프라인 시작
- Execution Fee 계산이 10퍼센트와 500 하한선을 정확 적용
- Landed Cost 계산에 1.15 버퍼 포함
- Verified 이후 핵심 값 수정 불가
- 새 Claim과 새 Verified 버전만 허용
- Slack 버튼과 큐 작업 idempotency 보장
- Free Analyze에서 고비용 외부 호출이 발생하지 않음

12.2 성능

- SOP 컨텍스트 캐시 참조
- H 리포트 목표 응답 7초 이내
- 크롤링과 OCR은 비동기

12.3 보안

- Signed URL 만료 적용
- 권한 없는 프로젝트 접근 차단
- 파일 업로드 정책과 무결성 적용

12.4 감사 추적

- Claim 생성, 변경, 승격, 반려가 audit_actions에 기록
- Evidence와 Claim 연결 추적 가능
- 상태 전이는 project_status_events로 재현 가능

12.5 쿠폰

- 코드 발급, 입력, 적립, 결제 적용, 사용, 롤백까지 원장으로 기록
- 최소 결제 1달러 유지

13 개발 티켓 묶음 마일스톤

M1 인프라와 인증

1. Firebase Auth 연동과 user 프로필 동기화

2. Cloud SQL 연결과 마이그레이션 규칙 dev stage prod
3. Secret Manager 주입
4. GCS 버킷과 Signed URL 업로드 조회
5. 비동기 큐 기본 워커

M2 데이터 코어 Claim Evidence Audit Resolution

6. projects 상태 머신, 전이 이벤트 기록, idempotency
7. sourcing_claims 불변 규칙, 단위와 통화 규칙
8. evidence_files 메타 저장, 업로드 정책
9. claim evidence 연결 로직
10. audit_actions 기록과 조회, Slack actor 매핑
11. Resolved View JSONB 스냅샷 생성과 갱신
12. Verified Snapshot 고정 저장과 PDF 재현

M3 AI와 파이프라인

13. SOP 컨텍스트 캐시 생성과 TTL
14. H 리포트 생성기, JSON 스키마 고정
15. OCR 추출 파이프라인, claim 생성
16. 크롤링 파이프라인, 공장 후보 claim 생성
17. Landed Cost 계산 모듈과 테스트

M4 결제 요청과 Slack 승인

18. Unlock 클릭 시 WAITING_PAYMENT 전환과 이메일 발송
19. Slack 결제 요청 알림 카드와 버튼
20. Slack 인터랙션
21. Confirm Payment 처리
22. Slack 중복 클릭 방지와 idempotency

M5 웹과 리포트

23. 유저 대시보드 프로젝트 리스트와 상태
24. 유저 리포트 H와 V 분리 렌더링, Resolved View 기반
25. Auditor Desk 조회 화면, 문서와 Claim Evidence Side by Side
26. Verified 리포트 PDF Export, 인장 포함

M6 쿠폰과 크레딧

27. 캠페인 생성 어드민 엔드포인트
28. 쿠폰 코드 생성과 일괄 발급
29. 쿠폰 코드 입력 검증, 계정당 제한과 만료
30. credits_ledger 적립, 사용, 롤백 처리
31. 결제 적용 UI, 최소 결제 1달러, 상한 규칙
32. 남용 방지, 리딤 제한, 레이트 리밋, 신호 기반 차단

Appendix 1 SOW Addendum v1.3

A 고객 커뮤니케이션 원칙

- 고객 화면과 메시지에는 1688, RapidAPI, 내부 소스명을 절대 노출하지 않는다
- 고객이 보는 가치는 전문가 검토와 검증 프로세스다
- Free Analyze 결과는 가설이며 실시간 공장 단가가 아니다
- Blueprint 이후에도 결과는 사람 검토와 승인 이후에만 고객에게 노출된다

B 비용 가드레일과 Phase별 외부 호출 규칙

Phase 1 Free Analyze

금지

- 1688 호출
- RapidAPI 호출
- 외부 OCR 호출

허용

- 모델 기반 추정
- 내부 기준표
- 캐시된 룰
- 스텁

Degrade 정책

- 비싼 호출이 필요해지는 순간 추정 불가로 내려가고 CTA만 보여준다

Phase 2 Blueprint 결제 승인 이후

허용

- 1688 호출
- RapidAPI 호출
- OCR 스텁 또는 실제 OCR

규칙

- 후보는 최소 20개 수집
- 내부에서 10개로 압축
- 자동 추천 금지
- 랭킹 금지
- 판단은 사람

Phase 3 Verified

규칙

- VERIFIED 자동화 금지
- Verified snapshot은 고정
- 수정은 새 버전으로만 가능

C 유저 입력 필드 규칙

Blueprint 요청 시 입력 필드

- quantity
- target price
- lead time
- special requirements

규칙

- 입력이 비어도 시작 가능
- 시작 시 system claim에 missing_fields 기록
- 운영자가 Slack 또는 이메일로 보완 요청

D 운영 플로우 원칙

- Blueprint 요청
- Start Blueprint 클릭 시 WAITING_PAYMENT 전환
- Slack 결제 요청 알림 발송
- 결제 승인
- Confirm Payment는 Slack에서만
- 승인 시 BLUEPRINT_RUNNING 전환
- blueprint pipeline enqueue
- 고객 커뮤니케이션
- 진행 중 메시지는 전문가 검토 진행 중으로 통일
- 내부 작업 상태와 소스는 공개하지 않는다

E 데이터 품질 기준

- 공장 후보 수집
- 최소 20개 수집

- 내부에서 10개만 남김
- 모든 자동 생성 값은 HYPOTHESIS claim으로만 저장
- 사람이 실행한 사실은 VERIFIED claim으로 기록
- 증거 없는 실행 기록 금지
- evidence id 필수

F 보안 및 시크릿 관리 원칙

- 모든 키는 환경변수로만 관리
- 저장소 커밋 금지
- 키 노출 의심 시 즉시 폐기 및 재발급
- Signed URL은 짧은 만료 유지
- admin 권한은 Firebase custom claim role로만 부여

G MVP 출시 Definition of Done 추가

사용자 플로우

- 사진 업로드 후 프로젝트 생성 가능
- report 화면 렌더링 가능
- blueprint 요청 가능
- WAITING_PAYMENT 전환과 사용자 안내 노출

운영자 플로우

- Slack 결제 요청 카드 수신
- Confirm Payment로 파이프라인 시작
- admin 화면에서 승인과 준비물 확인과 기록 가능

안전성

- idempotency 적용
- audit 로그가 모든 주요 액션에 남음
- Free Analyze에서 고비용 API가 호출되지 않음

Appendix 2 Launch Runbook v0.1

목표

- 첫 고객을 받아도 되는 상태를 빠르게 만들고 운영 사고를 줄인다

런칭 전 체크리스트

- Firebase
- Google 로그인 동작
- admin 계정 role 설정 완료
- Slack
- signing secret 설정

- bot token 설정
- payment channel id 설정
- interactivity url 연결
- DB
- migrate 실행 완료
- 기본 테이블 생성 확인
- Storage
- 버킷 존재
- 업로드 경로 규칙 확정
- Backend
- health endpoint 확인
- projects 관련 엔드포인트 정상
- transition 정상
- slack 관련 엔드포인트 정상
- Frontend
- 업로드 페이지에서 프로젝트 생성까지 완료
- blueprint request 페이지에서 transition 호출 완료
- admin 페이지에서 internal review 호출 완료

내부 테스트 시나리오

- 유저 로그인
- 사진 업로드
- report 이동 확인
- blueprint request 입력 후 시작
- Slack에서 결제 요청 카드 확인
- Confirm Payment 클릭
- admin에서 후보와 플랜 확인
- approve steps 실행
- execution action prepared 확인
- evidence id 입력 후 mark sent
- execution result가 한 번만 기록되는지 확인

운영 규칙

- 고객에게 소스명, 내부 링크, 1688 언급 금지
- 고객 메시지는 전문가 검토 중심으로 통일
- Verified 단계는 비가역 성격이 있으므로 버튼 주변에 경고 문구 유지

사고 대응

- 중복 클릭 또는 중복 실행
- idempotency로 차단되는지 audit로 확인
- 키 노출 의심
- 즉시 폐기 후 재발급

- 배포 환경변수 교체
- 교체 우선순위
    - Slack
    - Firebase
    - RapidAPI
    - Email

Appendix 3 Backlog

SOW Addendum 뒤에 붙이는 추가 백로그

- Free Analyze H Report 실제 구현
- 모델만 사용
- 내부 기준표 매칭으로 FOB, duty, margin 추정
- 비용 가드레일 테스트 추가
- Email 자동화
- WAITING_PAYMENT 진입 시 안내 메일
- Need more docs 시 요청 메일
- 진행 업데이트 템플릿
- File upload UX
- evidence 업로드 화면
- 업로드 후 evidence id 자동 입력
- Admin UX
- 후보 20개 표시 옵션
- 10개로 줄이는 체크리스트 화면
- 후속 내부 단계 트리거
- Verified 이후 수동 버튼으로 평가 실행
- eligible 결과를 admin 화면에 표시

Cursor 구현 프롬프트 영어 버전

Build the NexSupply AI driven factory verification MVP using Firebase Auth, Cloud Run, Cloud SQL Postgres, GCS signed URLs, Vertex AI Gemini, and Slack interactivity.

Implement an immutable claim based data model with evidence linking, audit actions, project status events, and resolved view JSONB snapshots.

Support user flow for Free Analyze, Blueprint payment request, Slack based Confirm Payment to start the Blueprint pipeline, and Final Verification with verified snapshot lock and PDF export.

Enforce cost guardrails for Free Analyze with no 1688, no RapidAPI, and no external OCR.

Degrade to unable to estimate and show CTA when expensive calls would be required.

Implement idempotency for Slack buttons, queue retries, and payment events.

Create milestones M1 through M6 as ticket groups and ship the MVP definition of done in the SOW.