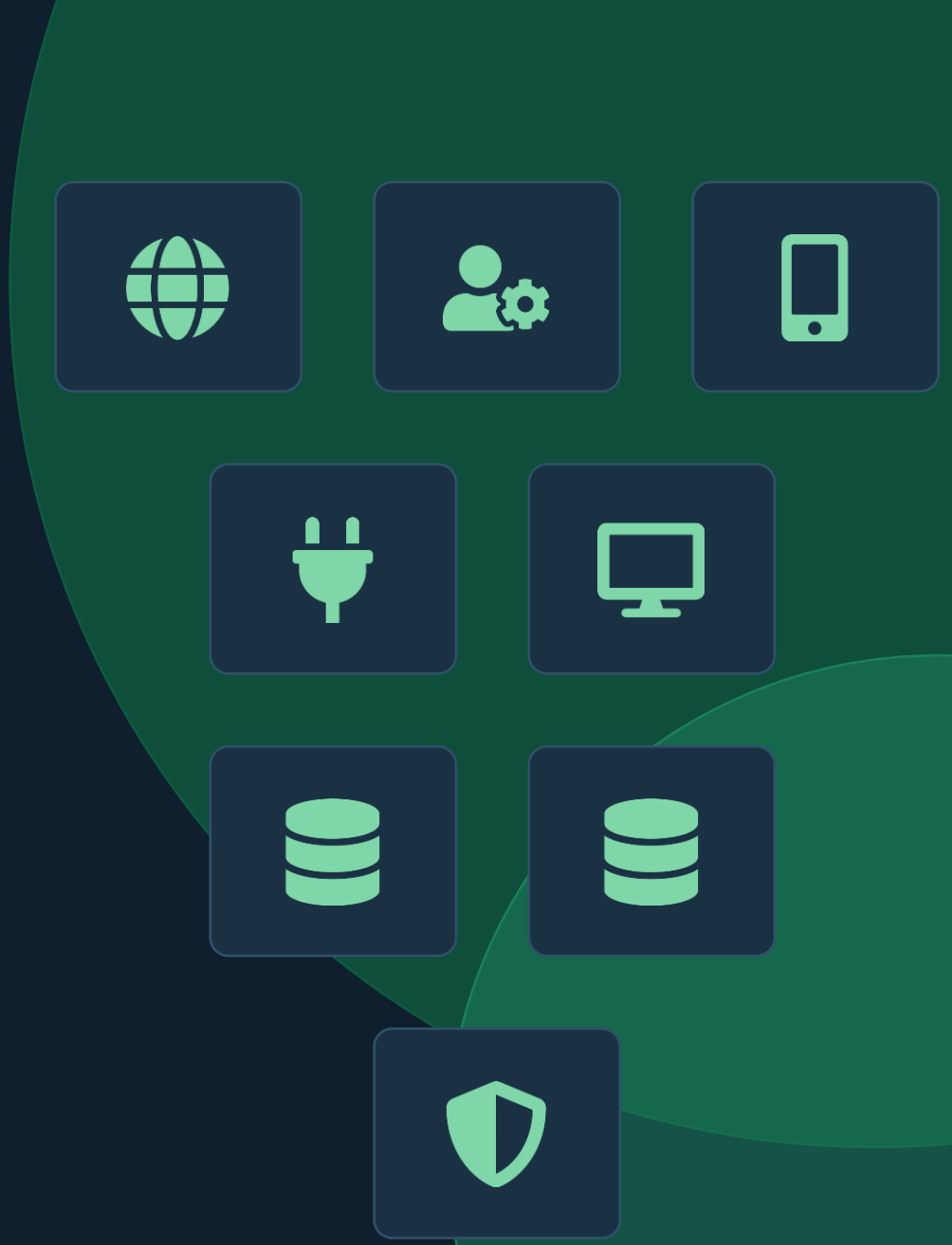
한국마트협회 · 기술 문서

MartLink

상용 운영 시스템 구성도

테스트 서버 한 대에서 개발 중인 시스템을 실제로 운영할 때의 구성입니다. 서버 분리 · 데이터베이스 이중화 · POS 연동 경로 · 유지보수 산정 항목까지 담았습니다.



서버 분리 | DB 이중화 | POS 연동 | 유지보수 산정

제작 한국마트협회 · 문서 판 1.0 · 2026년 9월

이 문서에 대하여

무엇을 담았고, 어떻게 읽는가

개발자가 구성을 파악하고, 협회가 **유지보수 비용을 항목별로 산정**할 수 있게 하는 것이 목적입니다.

01 ~ 02

전체 구성과 서버

전체 구성도 · 네트워크 구역 · **서버 목록과 권장 사양** · 계층별 상세

03

POS 연동 경로

협조 POS 의 **API 연동**과 비협조 POS 의 **매장 수집기** — 구성과 흐름

04

데이터 · 이중화

데이터베이스 이중화 · 백업과 복구 · 파일 저장소 · 재해 복구

05 ~ 06

운영과 유지보수 산정

보안 · 관측 · 배포 · **유지보수 비용 산정 항목** · 전환 작업

그림 읽는 법

- 서버 · 구성 요소
- 핵심 서비스
- 데이터 구역
- 외부 · 주의

사양과 수량은 「초기 권장」 입니다

회원 마트 수와 거래량은 파일럿에서 실측한 뒤 조정합니다. 이 문서의 수치는 **개발 환경 실측**과 **일반적인 상용 구성 관례**에서 나온 출발점이며, 단가는 비워 두었습니다.

01 전체 구성

지금의 테스트 서버와 상용 구성은 무엇이 다른가

지금은 **서버 한 대에 전부**가 올라가 있습니다. 개발에는 충분하지만, 한 곳이 멈추면 전부 멈춥니다.

항목	지금 (테스트 서버)	상용 운영 구성	왜 바꾸는가
서버	1대에 전부	시작 7대 — 웹 2 · DB 2 · 백업 · 관측 · AI	한 대의 고장이 전체 중단이 되지 않게
홈페이지 · 관리자 · 앱	한 프로그램이 주소로 갈라 응답	같은 WEB 2대에 함께 — 기준을 넘으면 역할을 떼어 냄	한 대가 멈춰도 다른 대가 이어받게
POS 연동	같은 프로그램 안	WEB 2대에 함께 — 수집이 화면을 늦추면 전용 서버로	수집 폭주가 화면을 느리게 하지 않게
데이터베이스	1대 (이중화 없음)	주 + 대기(대기가 읽기 조회 겸용)	고장 시 자동 전환 · 데이터 무손실
예약 작업	서버의 예약 기능	WEB 한 대에서만 (잠금)	두 대가 같은 작업을 겹쳐 돌지 않게
AI	바깥 AI 서비스 호출	자체 AI 서버 1대 (GPU)	상품 · 판매 자료가 바깥으로 나가지 않게
백업	같은 서버 안	별도 백업 서버 + 원격지 보관	서버가 죽으면 백업도 같이 죽지 않게
환경	개발 · 운영 겸용	개발 / 검증 / 운영 3벌	검증하지 않은 것이 운영에 가지 않게

프로그램은 **하나의 코드**입니다. 처음에는 WEB 2대에 역할을 함께 올리고, 잰 값이 기준을 넘는 역할만 떼어 냅니다 — 코드는 그대로입니다.

전체 시스템 구성도 — 상용 운영 (역할 그림)



01 전체 구성

네트워크 구역과 통신 허용 규칙

구역 사이의 문은 **필요한 방향으로만** 엽니다. 데이터 구역은 바깥에서 직접 닿을 수 없습니다.



출발	도착	포트 · 방식	비고
인터넷	경계 구역	443 (암호화)	80 은 443 으로 넘긴다
경계	서비스 구역	서버별 서비스 포트	서버는 공인 주소를 갖지 않는다
서비스	데이터 구역	DB 포트	인증서 고정 · 계정별 접속 수 제한
서비스 · 내부	외부 기관	443 (나가는 방향)	외부 연계 게이트를 거친다
매장 수집기	경계 구역	443 (나가는 방향)	들어가는 통신 없음 · 파일럿부터 MediBridge
관리자 PC	관리 구역	VPN → 접속 관문	직접 접속 금지 · 명령 기록

지표 조회 경로(/metrics)는 바깥에서 404 입니다. 내부 구역의 관측 서버만 읽습니다. 관리 화면 주소를 바깥에 여는 일도 없습니다.

운영 환경 — 시작 구성 7대, 잰 값으로 늘립니다

회원 마트 1,000곳까지의 구성입니다. 같은 빌드를 역할로 나누는 구조라 **웹 · 앱 · POS 수신 · 배치를 한 쌍에 함께** 올리고, 기준을 넘으면 역할을 떼어 냅니다.

서버	맡는 일	수량	CPU / 메모리	저장	이중화
WEB	부하 분산(가상 IP) · 홈페이지 · 관리자 · 앱 · POS 수신 · 배치	2	8코어 / 16GB	200GB	동시 운영 · 배치는 한 대만(잠금)
DB	주 · 대기 데이터베이스 — 대기는 통계 · aT 전송 조회 겸용	2	8코어 / 32GB	SSD 1TB	실시간 복제 · 자동 전환
BKP	백업 · 원격지 사본	1	4코어 / 8GB	4TB	원격지에 사본
OPS	관측 · 접속 관문 · 배포	1	4코어 / 16GB	500GB	단일 (서비스 무관)
AI	자체 LLM 추론 — GPU 48GB × 2 (매핑 4단 · 사진 읽기)	1	32코어 / 256GB	NVMe 2TB	단일 — 멈추면 4단이 기권
FILE	파일 저장소 — 증빙 · 업로드 원본 (객체 저장소)	1식	—	500GB~	저장소 자체 이중화

서버	CPU	메모리	GPU	서버 저장
7대	**72코어**	**376GB**	**48GB × 2**	**약 8.9TB**

늘리는 기준 — 잰 값이 넘을 때

웹 CPU 60% 이상이 1주

→ WEB 을 같은 구성으로 한 대씩 더

POS 수신이 화면 응답을 늦춤

→ POS 수신 전용 2대로 떼어 냄

통계 · aT 전송이 대기 DB 를 누름

→ 읽기 전용 복제본 1대 추가

WEB 4대 이상

→ 부하 분산 전용 장비(또는 클라우드 LB)

02

계층별 서버 구성

홈페이지 · 관리자 · 앱 · POS 연동은 역할이 다릅니다. 처음에는 WEB 2대에 함께 올리고, 잰 값이 기준을 넘는 역할만 떼어 냅니다.

홈페이지

배치 · 워커

관리자

같은 코드 · 역할별 배포

앱

02 계층별 서버 구성

홈페이지 · 관리자 · 앱 — 역할은 셋, 시작은 WEB 2대

셋은 **쓰는 사람도, 몰리는 시간도, 막아야 할 것도** 다릅니다. 처음에는 한 쌍에 함께 두고, 몰리는 역할부터 떼어 냅니다.

WEB-HOME

홈페이지 서버

시작은 WEB 에 · 떼면 2코어 / 4GB × 2

- 주소: 협회 홈페이지
- 공지 · 주요활동 · 자료실 · 안내 페이지
- 참여 신청 · 신청 진행 조회
- 로그인 없음 — 누구나
- 거의 읽기만 · 캐시 효과가 크다

공지 직후 방문이 몰려도 업무 화면은 멀쩡하다

WEB-ADM

관리자 서버

시작은 WEB 에 · 떼면 4코어 / 8GB × 2

- 주소: 운영 시스템
- 협회 운영 콘솔 · 지사 · 점주 포털
- 로그인 필수 · 역할과 지사로 범위 제한
- 돈과 자격을 바꾸는 쓰기가 많다
- 접속 기록 · 감사 이력 대상

가장 엄격하게 지킨다 — 접속 주소 제한도 걸 수 있다

APP-API

앱 서버

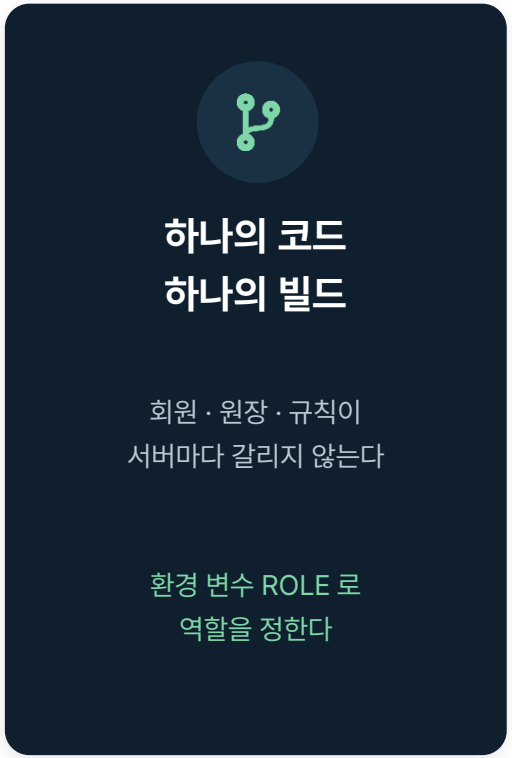
시작은 WEB 에 · 떼면 4코어 / 8GB × 2~

- 주소: 소비자 앱 · 모바일 웹
- 가격 비교 · 지도 · 장바구니 · 전단지
- 읽기는 대기 DB 를 본다(확장 시 복제본)
- 이용자 수에 비례해 증설
- 사진은 파일 저장소 · 캐시에서

이용자가 늘면 이 서버만 늘린다

코드는 하나, 배포는 역할별로

프로그램을 넷으로 쪼개지 않습니다. **같은 빌드 산출물**을 네 역할의 서버에 올리고, 각 서버는 자기 경로만 받습니다.



WEB-HOME	홈페이지 주소의 요청	/ /notice /docs /join /status
WEB-ADM	운영 시스템 주소의 화면	/gov/ **/mart/** /admin/** /api/gov /api/mart
APP-API	소비자 경로	/m/ **/api/m/**
POS-API	연동 경로	/api/auth/agent /api/agent/**

자기 역할이 아닌 경로는 **404** 로 답합니다(부하 분산기에서 한 번, 서버에서 한 번). 데이터 구조 변경(마이그레이션)은 배포 때 **WEB 한 대에서만** 실행합니다.

배치 · 워커 서버 — 예약 작업 목록

웹 서버의 재시작과 무관하게 돕니다. 2대 가운데 **한 대만 실행**하고, 그 서버가 죽으면 대기 서버가 이어받습니다.

작업	주기	하는 일	멈추면
무결성 검사	매일 04:05 (일요일은 전수)	원장 · 집계 · 지문 · 청구서를 다시 센다	36시간 뒤 정산 문이 닫힌다
AI 매핑 4단	매일 05:10	기권으로 남은 상품을 후보 안에서 다시 묻는다	심사 대기가 쌓인다
보존 기간 파기	매시 15분	기간이 지난 원문 · 보고 기록을 걷는다	저장 공간이 찬다
운영 알림	매시 45분	연동 중단 · 미처리 건을 담당자에게 알린다	장애를 늦게 안다
점주 알림	매일 08:30	배정 · 정산 · 심사 결과를 알린다	전화 문의가 는다
집계 갱신	수집 직후 (상시)	일별 집계를 새 실적에 맞춘다	화면의 집행액이 늦는다
전체 백업	매일 03:20	데이터베이스 전체를 뜬다	복구 지점이 멀어진다
증분 백업	4시간마다 40분	바뀐 부분만 뜬다	〃
논리 백업	매일 03:50	프로젝트 단위로 되돌릴 사본	부분 복구를 못 한다

⚠ 예약 파일의 줄바꿈 형식이 어긋나면 작업이 **오류 없이 실행되지 않습니다.** 설치 도구가 형식을 검사하고, 「돌았는지」를 관측 서버가 따로 확인합니다.

03

POS 연동 구성

협조하는 POS 는 API 로, 협조하지 않는 POS 는 매장에 설치하는 수집기로 — 두 길 모두 같은 연동 서버로 모입니다.

연동 구성도

API 연동 흐름

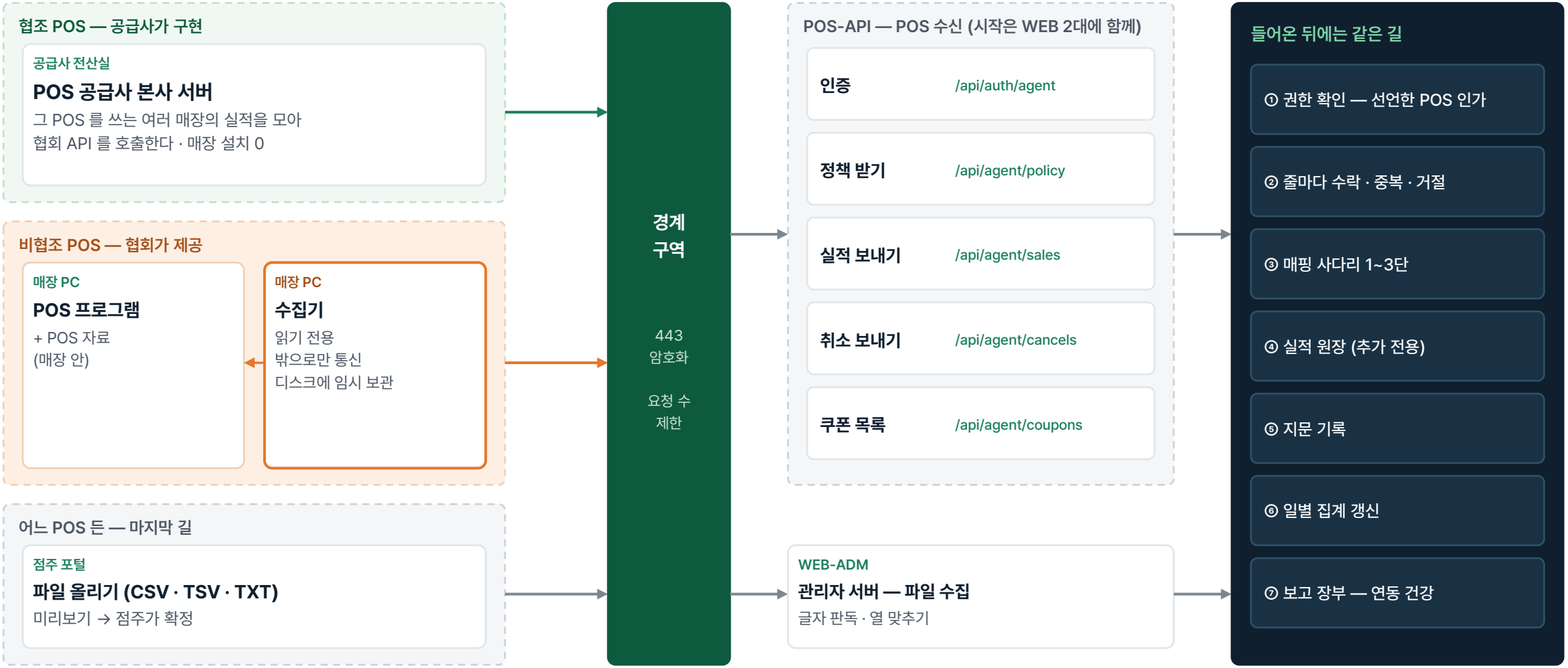
수집기 구성

수집기 흐름

방식 비교

연동 유지보수

POS 연동 구성도 — 세 갈래가 한 서버로 모인다



협조 POS — API 연동의 호출 순서

공급사는 **규격 문서 · 시험용 키 · 적합성 시험 도구**를 받아 구현합니다. 규격 이름은 martlink.agent.v1 입니다.

1	공급사 → 협회	발급받은 연동 키로 인증한다 → 30분짜리 세션
2	공급사 → 협회	정책을 받는다 — 농할 회차 · 대상 품목 · 한도 · 쿠폰 코드 · 개정 번호
3	공급사 → 협회	판매 줄을 보낸다 — 한 번에 1,000줄까지, 거래 열쇠 포함
4	협회 → 공급사	줄마다 수락 · 중복 · 거절을 갈라 답한다 (거절 사유 포함)
5	공급사 → 협회	취소가 생기면 취소 줄을 보낸다 — 원본은 지우지 않는다
6	공급사 → 협회	매장의 쿠폰 목록을 올린다 — 농할 판정은 협회가 한다
7	공급사 → 협회	세션이 끝나면 1번부터 — 정책 개정 번호가 바뀌면 다시 받는다

연동 키

협회 콘솔에서 발급 · 회수. 저장은 해시로만. 교체 기간에는 두 개가 함께 산다.

거래 열쇠

사업자번호 : 전표번호 : 라인번호. 같은 줄을 다시 보내면 「중복」으로 답한다.

적합성 시험

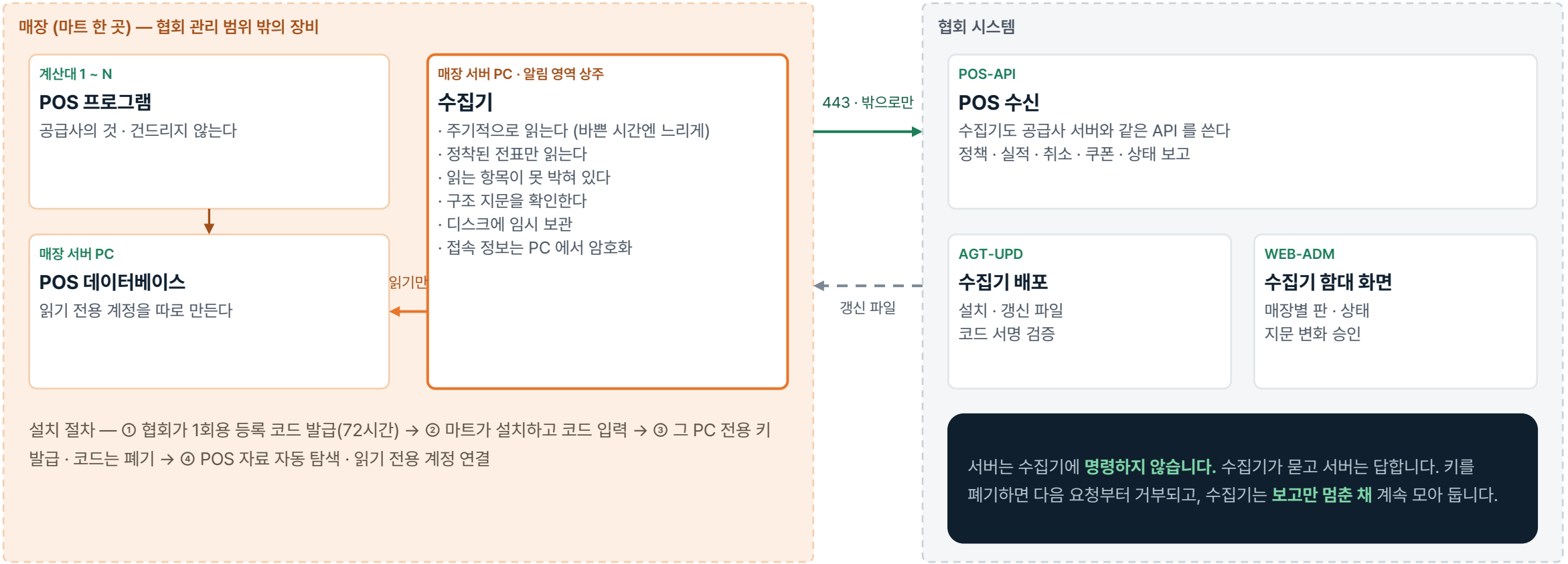
시험용 공급사(conformance)로 등록해 같은 도구로 양쪽이 확인한다.

요청 제한

경계 구역에서 키마다 요청 수를 제한한다. 넘으면 429.

비협조 POS — 매장 수집기의 구성

공급사가 협조하지 않으면 **협회가 만든 수집기**를 마트가 자기 매장 PC 에 설치합니다. 매장 쪽으로 들어가는 통신은 없습니다.



설치 절차 — ① 협회가 1회용 등록 코드 발급(72시간) → ② 마트가 설치하고 코드 입력 → ③ 그 PC 전용 키 발급 · 코드는 폐기 → ④ POS 자료 자동 탐색 · 읽기 전용 계정 연결

수집기의 한 주기와, 문제가 생겼을 때의 동작

우리 최악의 사고는 **「수집이 멈췄다」** 여야 하고, **「매장이 멈췄다」** 여서는 안 됩니다.

정상 주기

1. 구조 지문을 확인한다 — 지난번과 같은가
2. 마지막으로 읽은 자리부터 조금 겹쳐 다시 읽는다
3. 아직 정착되지 않은 전표는 다음 주기로 미룬다
4. 할인 금액을 상품 줄에 귀속시킨다
5. 디스크에 적는다 — 보내기 전에 먼저
6. 1,000줄씩 잘라 연동 서버로 보낸다
7. 수락된 줄만 비우고, 읽은 자리를 전진시킨다

일어난 일	수집기의 동작	협회가 보는 것
인터넷이 끊겼다	디스크에 쌓고 간격을 늘려 재시도	12시간 뒤 「조용함」
POS 구조가 바뀌었다	수집을 멈추고 알린다	지문 변화 승인 대기
디스크가 찼다	수집을 스스로 멈춘다	「멈춤」 + 사유
마감 합계가 어긋났다	보고하지 않고 알린다	대사 불일치 목록
키가 폐기되었다	보고만 멈추고 계속 모은다	키 상태 「폐기」
계산대 한 대가 단독 모드	그대로 보고한다	계산대별 마지막 거래 시각
매장 PC 가 꺼졌다	— (켜지면 이어서)	36시간 뒤 「멈춤」

연동이 멈춘 동안에도 점주는 **파일 올리기**로 실적을 낼 수 있습니다.

연동 방식 비교 — 유지보수 관점

같은 공급사가 **수집기에서 API 로 옮겨 가면** 협회의 유지보수 부담이 크게 줄어듭니다. 협회의 요청이 중요한 까닭입니다.

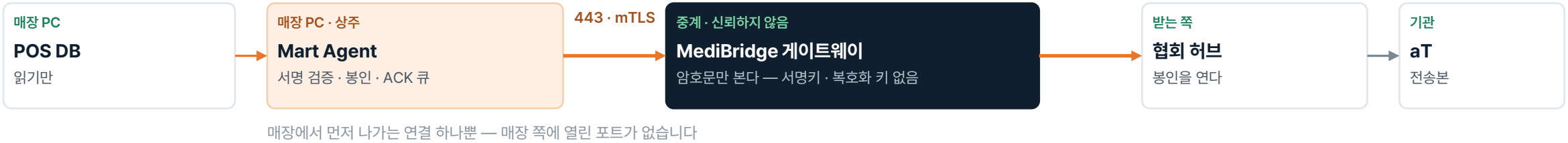
구분	API 연동 (협조 POS)	매장 수집기 (비협조 POS)	파일 올리기
구현 주체	POS 공급사	협회 (운영사가 제작)	점주
매장 설치	없음	매장마다 설치 · 갱신	없음
실시간성	공급사 주기 (분 단위)	수집기 주기 (분 단위)	점주가 올릴 때
POS 갱신의 영향	공급사가 흡수한다	지문 변화 → 협회가 대응	내보내기 형식이 바뀔 수 있다
현장 지원	거의 없음	설치 · PC 교체 · 백신 충돌	사용법 안내
협회 서버 부담	연동 서버	연동 서버 + 배포 서버 + 함대 관리	관리자 서버
유지보수 산정 단위	공급사 수	공급사 종류 수 + 설치 매장 수	문의 건수
보안 위험	낮다	매장 PC 의 상태에 달려 있다	낮다

수집기는 **공급사 종류마다 읽는 법이 다릅니다.** 비협조 공급사가 하나 늘면 읽는 법 한 벌과 그 공급사의 갱신을 따라가는 비용이 함께 늡니다.

보안 통신

MediBridge — 매장과 중앙을 잇는 보안 통신 계층

인바운드 포트 없이 내부 시스템을 중앙에 잇는 보안 통신 계층입니다(의료 연동에서 운영 중). **Mart Agent 는 지금 HTTPS 로 직접 보내고, 파일럿에서 이 터널 위로 옮깁니다.**



매장에서 먼저 나가는 연결 하나뿐 — 매장 쪽에 열린 포트가 없습니다

인바운드 포트 0

매장이 밖으로 먼저 연결(443 · WSS). 끊기면 재연결(백오프 · 하트비트)

기기 인증서

CA 발급 · 매장 ID 에 묶인 mTLS · 자동 회전 · 즉시 폐기

서명된 명령 · 정책

Ed25519 — 중계는 서명키가 없어 위조할 수 없습니다

종단 간 봉인

HPKE — 중계는 암호문만, 받는 쪽만 엽니다

재전송 · 중복 차단

nonce · 만료 시각 · 멱등 ID · ACK 큐(최소 1회 전달)

Agent 정책엔진

기본 거부 · 허용 목록 · 파라미터 검사(주입 차단)

감사

해시체인 감사 로그 — 개인정보는 남기지 않습니다

안전한 갱신

코드서명 검증 · A/B 업데이트 · 롤백

지금 — 의료 연동 운영 서버 가동 · 병원 2곳 연결(2026.7) · 자동 테스트 전부 통과. MartLink 의 Mart Agent 는 지금 HTTPS 로 허브에 직접 보내고, **파일럿에서 MediBridge 터널 위로 옮깁니다.**

보안 통신

왜 MediBridge 인가 — HTTPS 직접 전송으로 남는 틈

지금 Agent 는 HTTPS 로 직접 보냅니다. 전송 구간은 암호화되지만 **누가 보냈는지 · 받은 정책이 진짜인지 · 얼마나 빨리 닿는지**는 HTTPS 만으로 정해지지 않습니다.

필요한 것	지금 — HTTPS 직접	MediBridge 위에서	농할에 걸린 것
보낸 매장의 신원	발급받은 키 문자열 하나 — 키 파일이 복사되면 다른 PC 도 그 매장으로 보낼 수 있음	기기 인증서(mTLS) — 매장 ID 에 묶임 · 자동 회전 · 즉시 폐기	실적은 정산 청구의 증빙
정책 반영 속도	Agent 가 30분마다 물어봄 — 배정 소진 · 회차 변경이 최대 30분 늦게 닿음	상시 연결로 변경을 바로 알림 → Agent 가 즉시 다시 받음	소진 뒤의 할인은 인정되지 않음
받은 정책이 진짜인가	전송 구간만 보호 — Agent 가 정책 자체를 검증하지 않음	Ed25519 서명 — Agent 가 검증한 정책만 적용	지정품목 · 율 · 1인 한도
중계 구간의 원문	프록시에서 TLS 가 풀려 내부로 평문 전달	HPKE 봉인 — 중계는 암호문만, 허브만 엶	영수증 원문
프로그램 갱신	코드 서명 · 자동 갱신 없음 — 매장마다 손으로 설치	코드서명 검증 · A/B 갱신 · 롤백	수천 대를 같은 판으로
감사	서버 접속 로그	해시체인 감사 로그 — 이력을 고치면 드러남	전송 · 정책 수신 이력

그대로 지키는 것 — 매장으로 들어오는 포트 0 · 서버는 Agent 에 명령하지 않음(정책엔진 기본 거부) · POS 에 쓰지 않음

새로 만들지 않는 이유 — 같은 문제(인바운드 포트 없이 내부 시스템을 중앙에)를 의료 연동에서 운영 중 · 병원 2곳 · 자동 테스트 전부 통과(2026.7)

04

데이터 구성과 이중화

정산 원장은 잃어서는 안 되는 데이터입니다. 주 서버가 죽어도 대기 서버가 이어받고, 서버가 통째로 사라져도 원격지의 백업에서 되살립니다.

DB 이중화

읽기 분리

백업과 복구

원격지 사본

용량 산정

데이터베이스 이중화 — 주 · 대기 · 읽기 전용

주 서버가 멈추면 대기 서버가 **자동으로 승격**합니다. 서비스 서버는 **한 개의 접속 주소**만 알면 됩니다.



자동 전환

감시자 셋(DB 2대 + 백업 서버)이 다수결로 판정한다. **수십 초 안에** 대기 서버가 주가 된다.

데이터 무손실

대기 서버가 받았다고 답한 뒤에 저장이 끝난다. **정산 데이터는 한 줄도 잃지 않는다.**

두 주인 방지

옛 주 서버가 되살아나도 **쓰기를 받지 못하게** 막는다. 원장이 둘로 갈리지 않는다.

복제 지연 감시

읽기 복제본이 늦으면 관측 서버가 알리고, 돈에 닿는 조회는 **주 서버**에서 읽는다.

백업과 복구 — 목표와 방법

이중화는 **장비 고장**을 막고, 백업은 **잘못 지운 것 · 망가진 데이터**를 되돌립니다. 둘은 서로를 대신하지 못합니다.

1분

복구 시점 목표

변경 기록을 1분 단위로 백업 서버에 보낸다

1시간

복구 시간 목표

백업에서 새 서버를 세우는 데 걸리는 시간

5년

정산 증빙 보존

청구 · 전송 · 감사 이력은 자동으로 지우지 않는다

백업 종류	주기	보관	쓰임
전체 백업	매일 03:20	3벌	서버를 통째로 되살린다
증분 백업	4시간마다	6벌	전체 백업 사이를 메운다
변경 기록	1분마다	전체 백업 기간만큼	임의 시점으로 되돌린다
논리 백업	매일 03:50	30일	표 · 프로젝트 단위로 되돌린다
원격지 사본	매일	30일 이상	전산실 자체가 사라졌을 때

복구를 해 본 백업만 백업이다

분기마다 **실제로 복구**해 원본과 견줍니다. 개발 환경 리허설에서는 복원본이 원본과 일치했습니다.

백업은 관리 계정만

서비스 계정은 백업 명령을 낼 수 없습니다. 백업 저장소는 **쓰기 전용**에 가깝게 둡니다.

파일도 함께

전단지 사진 · 서류 · 자료실 문서는 파일 저장소의 **판 관리와 복제**로 지킵니다.

용량 산정의 근거

추정이 아니라 **개발 환경에서 잰 수**에 회원 규모를 곱한 값입니다. 회원 수가 정해지면 식에 넣어 다시 셉니다.

항목	잰 값 · 가정	출처
마트 한 곳의 하루 거래 줄 수	약 2,600줄 (중앙값) · 상위 10% 는 16,000줄	개발 환경 실측
원장 한 줄의 크기 (색인 포함)	약 570바이트	원장 503만 줄 실측
지문 기록	원장의 약 14%	〃
수집 속도	1,000줄 묶음 0.2초	〃
무결성 전수 검사	714만 행 16초	운영 서버 실측
가장 큰 청구 한 건	146,715줄 접기 0.7초	〃
보존 기간	원문 90일 · 원장 1년 · 집계와 증빙 5년	보존 정책

회원 마트 1,000곳으로 셈하면

하루 거래 줄	**260만 줄**
하루 원장 증가	**약 1.7GB**
1년 원장 (지문 포함)	**약 620GB**
수집 피크	**초당 수백 줄**

농할 대상 품목만 받으면 이보다 훨씬 작습니다 — 구독이 수집 범위를 정합니다.

SSD 1TB 는 **회원 1,000곳 · 전 품목 수집** 기준 1년분입니다. 3,000곳이면 저장 공간을 늘리거나 원장을 기간별로 나눕니다(데이터베이스 분할).

05

운영 구성

서버를 세우는 것보다 돌리는 것이 어렵습니다. 밖과의 연결 · 보안 · 관측 · 배포 · 장애 대응을 구성으로 정해 둡니다.

외부 연계

보안 구성

관측과 알림

배포와 환경

장애 대응

05 운영 구성

외부 기관 · 서비스와의 연계

밖으로 나가는 통신은 **외부 연계 게이트** 한 곳을 지납니다. 상대가 멈춰도 우리 화면이 멈추지 않게 합니다.

상대	무엇을 주고받나	방향	과금	멈추면	지금 상태
aT	정산 전송본 · 증빙 파일	나감	없음	장부에 실패로 남고 다시 보낸다	기관 API 규격 대기 — 파일 제출은 가능
지도 · 좌표	주소 → 좌표 · 지도 표시	나감	호출량	지도 없이 목록으로 보인다	도메인 등록 필요
AI	매핑 4단 · 전단지 읽기	내부 (자체 서버)	장비 (월 고정)	기권으로 남아 사람이 본다	GPU 서버 1대 · 모델 후보 정함
알림 · 문자	점주 · 담당자 알림	나감	건수	화면의 알림함에 남는다	채널 미정
결제 대행	마트페이 승인 · 정산	양방향	수수료	— (마트페이 미개발)	정책 결정 대기
POS 공급사	실적 · 쿠폰 (연동 API)	들어옴	없음	「조용함」 → 「멈춤」 으로 드러난다	규격 · 시험 도구 완성

외부 키는 봉함해 보관

키 원문은 암호화해 저장하고 **화면 · 기록 어디에도 새지 않게** 합니다. 배포 없이 교체합니다.

기다리는 시간을 못 박는다

상대가 늦으면 **정해진 시간에 끊고** 다음 길로 갑니다. 화면이 함께 멈추지 않습니다.

호출을 전부 적는다

사용량 · 시간 · 성패를 기록합니다. **과금 서비스의 청구서와 대조**할 수 있습니다.

05 운영 구성

자체 AI — 무엇을 하고, 어떤 장비가 필요한가

AI 는 **마트마다 다른 상품명을 정부 표준품목에 잇는 일**을 돕습니다. 협회 서버 안에서 돌려 **상품 · 판매 자료가 바깥 AI 회사로 나가지 않습니다.**

① AI 가 하는 일

상품명 잇기

예) 「햇사과부사5kg특」 → 표준품목 「사과(후지)」 — 후보 8개 중에서만 고르고, 확정은 사람

사진 읽기

전단지 사진에서 상품과 가격을 읽어 입력을 덜어 줌

문의 답변 (나중에)

소비자 질문에 답하기 — 지금은 열지 않음

② 언제 AI 를 부르나

다시 팔린 상품

이미 매핑된 상품(마트 × 상품코드)은 판정을 다시 하지 않음 — AI 도 규칙도 돌지 않음

처음 보는 상품

들어오는 순간 규칙 3단(정확 · 별칭 · 유사)으로 판정 — AI 없음

규칙이 못 잇은 것만

매일 05:10 · 후보가 있는 것만 AI 에 — 지금은 한 판 50건으로 묶어 둠

③ 실제 쓰임과 장비

운영 실측

12일(9.26~10.7) 135회 · 하루 3~18회 — 지금은 바깥 AI 로

AI 서버 1대

AI 전용 그래픽 카드(48GB) 2장 — 1장은 글, 1장은 사진

멈추면

사람이 대신 확인 — 정산은 그대로 진행

승인된 상품명은 별칭 사전에 남아 다른 마트의 같은 이름도 AI 없이 잡습니다 · 같은 상품코드에 이름이 바뀌면 협회가 다시 확인하고, 그때까지 바뀐 뒤의 판매는 정산에서 보류합니다

모델 후보 — 글 Qwen3-32B · 사진 Qwen3-VL-32B (Apache 2.0) · NVIDIA L40S 48GB × 2

자체 AI — 3,000곳 운영 · 하루 20곳 신규에도 충분합니다 (예상)

AI 는 판매를 세지 않고 **상품을 한 번씩 판정**합니다. 운영 중인 마트는 매핑이 끝나 **새 상품만** 묻고, 하루 질문의 대부분은 **새로 들어온 마트의 첫 연결**입니다.

하루에 AI 에 묻는 상품 수

항목	셈	AI 질문 수
기존 3,000곳의 새 상품	3,000곳 × 하루 20개 × 3%	약 1,800건
신규 20곳의 첫 연결	20곳 × 95,000개 × 3%	약 57,000건
합계		**약 58,800건**
카드 1장(글)이 걸리는 시간	58,800건 ÷ 초당 5건	약 3시간 16분
밤 6시간에 처리할 수 있는 양	초당 5건 × 6시간	108,000건

1건 = 상품 하나를 AI 에 한 번 묻는 것(「이 상품명은 표준품목 후보 8개 중 무엇인가」) — 판매 · 영수증 건수가 아닙니다

결과

여유 약 46%
카드 1장으로 밤 6시간 안에
질문 58,800건 — 약 3시간 16분

하루 약 37곳
카드 1장이 받는 신규
기존 3,000곳을 돌리면서도

사진 전용
카드 2장째
전단지 · 사진 읽기 · 몰리면 글도 거듦

가정 (파일럿에서 잼)

마트 한 곳 상품 약 95,000개(시범 매장 실측) · AI 까지 가는 비율 3%(프로토타입 값) · 운영 중 마트의 새 상품 하루 20개 · 카드 1장 초당 5건(보수적) · 밤 6시간(한 판 50건 묶음은 올림)
같은 상품명이 다른 마트에서 재사용되는 효과를 넣지 않은 최악의 셈입니다 — 실제로는 신규 마트의 AI 일이 이보다 줄어듭니다.

보안 구성 — 여섯 겹

한 겹이 뚫려도 다음 겹이 막습니다. 정산 데이터는 **관리자 계정으로도** 고치거나 지울 수 없습니다.

1 경계

방화벽 · 웹 방화벽 · 요청 수 제한. 바깥에 열린 포트는 **443 하나**입니다.

2 통신

전 구간 암호화. 데이터베이스 접속도 **인증서를 고정**해 암호화합니다.

3 접근 통제

역할 넷 + 지사 범위. 화면이 그려지기 **전 단계**에서 막아 내용이 새지 않습니다.

4 데이터

서비스 계정은 관리자 권한이 없습니다. 원장 · 이력은 **추가만** 됩니다.

5 개인정보

거래 자료의 회원번호 · 카드 정보는 **읽지 않습니다.** 계좌번호는 가려서 기록합니다.

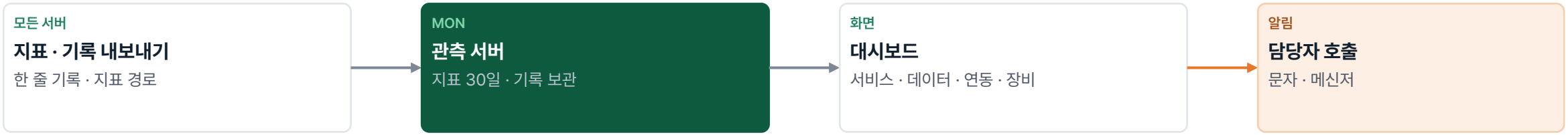
6 감사

누가 · 언제 · 무엇을 · 왜. **5년 보존**, 관리 구역 접속 명령도 기록합니다.

정기 점검 항목 — 취약점 점검(연 1회 이상) · 인증서 갱신(자동, 만료 30일 전 알림) · 계정 · 키 정리(분기) · **방어가 실제로 걸려 있는지 직접 지워 보는 검사**(배포마다)

관측과 알림 — 무엇을 보고, 언제 깨우는가

알림을 많이 만들면 아무도 보지 않습니다. **사람을 깨우는 것**과 **화면으로 보는 것**을 가릅니다.



구분	신호	기준	대응
즉시 호출	서비스 중단 · 데이터베이스 중단	1분 이상 응답 없음	당번이 즉시 확인
즉시 호출	무결성 검사 실패	검사 결과 불일치	정산 문이 닫힌다 · 원인 조사
즉시 호출	복제 끊김 · 백업 실패	지연 1분 초과 · 백업 1회 누락	이중화 상태 복구
업무 시간	연동 중단 매장 증가	36시간 무보고 매장	매장 · 공급사에 연락
업무 시간	매핑 승인 대기 누적	대기 비율 기준 초과	담당자 승인
업무 시간	디스크 · 메모리 · 접속 수	80% 초과	증설 검토
화면만	응답 시간 · 요청 수 · 외부 호출량	—	추세를 본다

환경 세 벌과 배포 절차

검증하지 않은 것이 운영에 가지 않습니다. 배포는 **한 대씩 교체**해 서비스가 끊기지 않습니다.

개발

지금의 테스트 서버 1대

시연 데이터 · 자유롭게 깨뜨린다

검증

한 대에 전 구성

운영과 같은 판 · 실 데이터의 가린 사본

운영

시작 7대 + 저장소

실 데이터 · 승인된 것만 올라간다

코드 병합

단위 검사 2,702건 통과

빌드

이미지 한 개 · 판 번호

검증 배포

검증 환경에서 실측

구조 변경

되돌림 점검 후 적용

순차 교체

한 대씩 · 상태 확인

운영 확인

운영 주소에서 실측

되돌리기 — 프로그램은 앞 판의 이미지로 한 줄에 되돌립니다. **데이터 구조 변경은 되돌릴 수 없으므로** 더하기만 하고(칸 삭제 · 형식 변경 금지), 적용 전에 「돌려만 보는」 점검을 거칩니다. 배포는 예약 작업 시각(03~05시)과 겹치지 않게 합니다.

무엇이 죽으면 무슨 일이 일어나는가

구성도에서 **한 곳만 죽어도 전체가 멈추는 자리**를 없앴는지 확인하는 표입니다.

죽는 것	서비스 영향	자동 조치	사람이 할 일	복구 목표
WEB 1대	없음	가상 IP 가 다른 대로 옮겨 감 · 배치는 남은 대가 이어받음	원인 확인 · 재기동	1분
주 데이터베이스	수십 초 쓰기 불가	대기 서버 자동 승격	옛 주 서버를 대기로 재편입	1분
대기 데이터베이스	없음 (이중화 풀림)	—	재구축 · 그동안 복제 없음 주의	4시간
자체 AI 서버	매핑 4단이 기권 · 사진 읽기 멈춤	사람 검토로 넘어감	재기동 · 밀린 건 다시 돌림	정산 영향 없음
파일 저장소	사진 · 문서 안 보임	저장소 자체 이중화	—	저장소 기준
외부 서비스	그 기능만 내려앉음	시간 제한 · 우회	상대에 확인	—
전산실 전체	전면 중단	—	원격지 백업에서 재구축	재해 복구 계획

관측 · 접속 관문 · 배포 서버는 단일 구성입니다 — 죽어도 서비스는 돌고, 그동안 **보지 못하고 배포하지 못할** 뿐입니다.

06

유지보수 산정

구성도에서 비용이 나오는 자리를 넷으로 나눴습니다. 수량과 산정 단위를 적고, 단가는 비워 두었습니다.

인프라

POS 연동

소프트웨어 · 외부 서비스

전환 작업

운영 업무

확정 필요 사항

06 유지보수 산정

유지보수 비용은 네 갈래에서 나온다

이 문서의 구성도를 **수량 × 단가**로 바꿀 수 있게 갈래마다 산정 단위를 정했습니다.

① 인프라

서버 · 회선 · 저장소

운영 7대(AI 서버 포함) + 검증 1대 + 저장소. **월 고정비.** IDC 라면 상면 · 회선 · 장비 감가, 클라우드라면 사용료.

② 외부 서비스

쓴 만큼 내는 것

지도 · 알림 · 인증서 · 도메인. **사용량에 비례.** AI 는 자체 서버라 ① 에 듭니다. 소프트웨어 사용료는 없습니다(전부 공개 소프트웨어).

③ 운영 업무

사람이 하는 일

감시 · 배포 · 백업 점검 · 장애 대응 · 문의 응대. **공수(인월)로 산정.**

④ POS 연동

공급사와 매장 수에 비례

수집기는 **공급사 종류마다 한 벌**, 설치 매장마다 현장 지원. 가장 변동이 큰 갈래입니다.

산정에 앞서 정해야 하는 세 가지

- 회원 마트 수 (1차 · 목표)
- IDC 와 클라우드 중 어느 쪽인가
- 서비스 수준 — 몇 시간 안에 복구하는가

① 인프라 · ② 외부 서비스 — 산정표

단가 칸은 비워 두었습니다. 견적을 받아 채우면 **월 고정비와 변동비**가 나옵니다.

갈래	항목	수량	산정 단위	단가	비고
①	WEB 서버 (8코어 / 16GB)	2대	대 / 월		홈페이지 · 관리자 · 앱 · POS 수신 · 배치 함께
①	데이터베이스 서버 (8코어 / 32GB / SSD 1TB)	2대	대 / 월		주 · 대기(읽기 겸용)
①	AI 서버 (32코어 / 256GB · GPU 48GB × 2)	1대	대 / 월		자체 LLM — 매핑 4단 · 사진 읽기
①	웹 방화벽	1식	식 / 월		장비 또는 서비스형 · 부하 분산은 WEB 의 가상 IP
①	백업 · 관측(접속 관문 · 배포 겸) 서버	2대	대 / 월		
①	파일 저장소 · 백업 저장 공간	4.5TB~	GB / 월		원격지 사본 포함
①	검증 환경	1대	대 / 월		한 대에 전 구성
①	회선 · 상면 또는 통신량	1식	식 / 월		IDC 는 상면 · 회선, 클라우드는 통신량
②	지도 · 좌표 서비스	—	호출 건 / 월		무료 구간 초과분
②	알림 · 문자	—	건 / 월		채널에 따라 다름
②	도메인 · 인증서 · 코드 서명	각 1	건 / 년		수집기 배포에 코드 서명 필요

소프트웨어 사용료는 **0** 입니다 — 운영체제 · 데이터베이스 · 웹 서버 · 관측 도구 모두 공개 소프트웨어입니다. 기술 지원 계약을 원하시면 별도 항목입니다.

③ 운영 업무 — 사람이 하는 일의 목록

공수 산정의 근거가 되는 업무 목록입니다. **주기 × 1회 소요 시간**으로 월 공수를 냅니다.

구분	업무	주기	산정 기준
상시	관측 화면 확인 · 알림 대응	매일	당번제 · 업무 시간 / 24시간 여부
상시	점주 · 협회 문의 응대 (기술)	수시	문의 건수
정기	보안 갱신 · 운영체제 갱신	월 1회	서버 대수
정기	백업 복구 리허설	분기 1회	회당
정기	계정 · 연동 키 정리 · 접속 기록 검토	분기 1회	회당
정기	취약점 점검 · 개인정보 점검	연 1회 이상	회당
정기	용량 점검 · 증설 계획	분기 1회	회당
수시	프로그램 배포 (기능 개선 · 오류 수정)	월 2~4회	배포 횟수
수시	장애 대응 · 원인 보고서	발생 시	건당 · 등급별
수시	농할 회차 개시 · 정산 마감 지원	회차마다	연 5~6회
수시	표준품목 · 규정 변경 반영	변경 시	건당

기능 개선은 별도

유지보수는 **지금 있는 것을 돌리고 고치는 일**입니다. 새 화면 · 새 서비스(마트페이 등)는 개발 과제로 따로 산정합니다.

정산 마감일은 다르다

회차 마감 전후에는 **배포를 멈추고** 대기 인력을 둡니다. 연 5~6회, 회차마다 며칠입니다.

④ POS 연동 — 가장 변동이 큰 갈래

비협조 공급사를 **수집기로 계속 둘 때**와 **API 로 옮겼을 때**의 유지보수 항목이 이만큼 다릅니다.

항목	산정 단위	API 연동	매장 수집기
연동 규격 유지 · 시험 도구	1식	필요	필요
공급사 기술 지원 (질의 응답)	공급사 수	필요	—
수집기 프로그램 유지 (읽는 법)	공급사 종류 수	—	필요
POS 갱신 추적 · 지문 변화 대응	공급사 종류 수 × 갱신 횟수	—	필요
수집기 배포 · 갱신 · 코드 서명	1식	—	필요
설치 지원 (원격 · 방문)	신규 설치 매장 수	—	필요
현장 장애 (PC 교체 · 백신 충돌)	설치 매장 수 × 발생률	—	필요
연동 건강 감시 · 매장 연락	연동 매장 수	적다	많다
농할 쿠폰 지정	신규 쿠폰 수	필요	필요

협회의 요청이 곧 비용 절감

공급사가 API 를 수용하면 오른쪽 열의 **여섯 항목이 사라집니다.**

산정 전에 알아야 하는 수

- 회원 마트가 쓰는 **POS 종류와 비율**
- 그중 **협조 가능한** 공급사
- 수집기를 설치할 **매장 수**
- 매장 PC 의 **운영체제 분포**

06 유지보수 산정

서비스 수준에 따라 비용이 달라진다

「몇 시간 안에 고치는가」가 인력 구성을 정합니다. 협회가 **등급을 고르시면** 공수가 나옵니다.

구분	기본	표준 (권장)	강화
대응 시간	평일 업무 시간	평일 업무 시간 + 회차 마감 기간	24시간 · 365일
장애 접수 → 착수	4시간 안	1시간 안	30분 안
서비스 복구 목표	다음 영업일	4시간	1시간
가동률 목표	—	99.5%	99.9%
정기 점검	분기	월	월 + 상시 감시
배포	월 1회	월 2~4회	수시
보고	분기 보고서	월간 보고서	월간 + 장애마다 원인 보고
맞는 시기	파일럿	농할 회차 운영	소비자 앱 전면 공개 뒤

가동률 99.5% 는 **한 달에 약 3시간 반**, 99.9% 는 **약 43분**의 중단을 허용한다는 뜻입니다. 구성도의 이중화는 99.9% 를 감당할 수 있게 짰습니다.

06 유지보수 산정

지금의 테스트 서버에서 상용 구성으로 — 전환 작업

구성도가 그림으로 끝나지 않으려면 **프로그램 쪽에서 해야 할 일**이 있습니다. 개발 과제로 산정하실 항목입니다.

#	작업	지금	해야 할 일	규모
1	역할별 배포	한 프로그램이 전부 응답	역할 설정에 따라 자기 경로만 받게 한다	중
2	읽기 · 쓰기 접속 분리	접속 주소 하나	소비자 조회 · 통계는 대기 DB 로 보낸다	중
3	예약 작업 잠금	서버의 예약 기능	WEB 두 대 중 한 대만 돌게 잠근다	소
4	파일 저장소 공유	서버의 디스크	여러 서버가 같은 저장소를 본다	소
5	요청 수 제한	서버 1대 기준	여러 서버가 같은 계수기를 본다	소
6	데이터베이스 이중화	1대	복제 · 자동 전환 · 접속 관문 구축	대
7	수집기 배포 체계	수동 설치	설치 프로그램 · 자동 갱신 · 코드 서명	대
8	자체 AI 서버	바깥 AI 서비스	GPU 서버 · 모델 설치 · 주소와 모델 이름만 바꿈 · 정확도 재기	중
9	이관 리허설	—	데이터 이관 · 주소 전환 · 되돌리기 연습	중

세션은 **서명된 쿠키**라 서버가 늘어도 공유 저장소가 필요 없습니다 — 서버 분리에서 가장 흔한 걸림돌이 이미 없습니다.

다음 걸음

견적을 내기 전에 정해 주실 다섯 가지

회원 마트 수	1차 개통 규모와 목표 규모. 저장 공간과 앱 서버 대수가 여기서 나온다
IDC 인가 클라우드인가	공공 · 정부 사업 데이터의 보관 위치 규정을 함께 확인
POS 분포	회원이 쓰는 POS 종류와 협조 여부. 수집기 설치 매장 수가 여기서 나온다
서비스 수준	기본 · 표준 · 강화 가운데 어느 등급인가
재해 복구 범위	원격지 백업까지인가, 원격지 대기 시스템까지인가

이 다섯이 정해지면 산정표의 수량이 확정되고, 단가를 넣어 **월 유지보수비**를 낼 수 있습니다.

제작 한국마트협회 · 문서 판 1.0