

과제 ⑧ 소액 RTGS Active-Active 구축 시 핵심 기술·운영 이슈 및 대응방안

소액 RTGS(신속자금이체) Active-Active 구축의 핵심 기술·운영 이슈 및 대응방안 한국은행 회계결제시스템 현대화 컨설팅 — 별도 트랙(한은금융망 결제 아키텍처 자체 변경) (v2.0 — 근거리 3센터 A-A-A-저널 순차처리 반영본)

목 차

0. 한 줄 요약 (Executive Summary)
 1. 과제 배경과 핵심 도전
 2. 핵심 기술 이슈와 대응방안
 3. 핵심 운영 이슈와 대응방안
 4. 국제 벤치마크 종합 — 무엇을 베끼고, 무엇을 못 베끼나
 5. 종합 — 대응방안 우선순위·이행 시사점
 6. 향후 추가 검토 고려 사항
- 부록 A. 모의 시뮬레이션 검증 결과

0. 한 줄 요약 (Executive Summary)

소액결제(인터넷·모바일뱅킹, 간편송금)를 **이연차액결제(DNS)** → **실시간총액결제(RTGS)**로 전환하면서, 그 신규 인프라를 **24시간 365일 무중단 Active-Active**로 구축할 때 직면하는 핵심 이슈를 식별하고 대응방안을 제시한다.

왜 만드나 두 축: ① **신용리스크 제거**(정산 시차에 쌓이는 외상 → 디지털 뱅크런 차단) ② **단일 실패점 해소**(현행 전자금융공동망 = 단일 운영기관 SPOF → "한 곳이 죽어도 안 멈추는" 다중화). 단, 현행망을 한 번에 대체하지 않고 **상당기간 병행 운영**하여 두 시스템이 서로의 대비책이 되게 한다 — 병행 자체가 SPOF 해소의 안전한 이행 수단이다(5.3-③).

핵심 도전 — 거래결제와 정반대: 거래결제는 "절대 못 쪼개는" 다자간 동시처리가 심장이지만, 소액 RTGS는 **건별 독립**이라 다중센터 동시가동(Active-Active)이 자연스럽게 성립한다. 단 24/365라 사람이 판단할 시간이 없어 "**결정도 자동**"으로 한 발 더 나아가야 하며, 도구를 잘못 쓰면(원장을 메시지 큐·조회DB로 동기화) **이중지급**이 난다.

정합성의 핵심 — "동기화"가 아니라 "하나의 순서를 셋이 재생": 여러 센터의 장부를 사후에 맞추려 하면 어긋난다. 대신 모든 거래를 **입구에서 하나의 전역 순번으로 줄 세우고(저널), 그 명단을 세 센터가 같은 순서로 재생**한다(유럽 TIPS·미국 FedNow의 방식). 이 구조가 이중지급·순서변경을 어떻게 원천 차단하는지는 2.3-부속에서 정면 검증한다.

핵심 권고 5줄

1. **복원력 골격: 근거리 3센터 Active-Active-Active + 저널 순차처리 + 정족수 자동전환** — RTO≈0(무복구 인계)·RPO 0. "5분"은 목표가 아니라 넘으면 안 될 **절대 상한선(레드라인)**. 유럽 TIPS의 3센터 A-A-A(RTO=0 실증)를 벤치마킹한다.
 2. **제3센터 확보(★⑧ 전용):** RTO≈0은 홀수 정족수(근거리 동기 3센터)라야 성립 → 광고·강남에 더해 **제3 근거리 동기센터**가 필수. **1순위 남대문 본점 자체 구축 / 2순위 수도권 IDC 임차**. + 대전 원거리 DR(광역재해 최후보루). **이 제3센터는 소액 RTGS 전용이며 회계결제(거액) 3센터와 별개다.**
 3. **원장 정합성:** 강한 일관성으로 원장 확정. **메시지 큐(입구)·강한일관성 원장·조회DB(사본)로 역할 분리** — 원장 동기화에 메시지 큐·조회DB를 쓰면 이중지급(절대 금기).
- **신기술은 "쓰느냐"가 아니라 "어디에 쓰느냐"의 문제다** — 같은 기술도 입구·조회엔 약이 되고 원장(돈을 확정하는 심장부)엔 독이 될 수 있다. 인메모리·NoSQL·API·공용 클라우드를 경로별로 가려 적용하며(상세·용어 풀이는 2.6), 신기술을 "쓰면 다 된다"는 식으로 과대포장하지 않는다.
1. **성능 목표:** 현행 피크(약 2,000 TPS 미만)를 기준선으로 하되, 절대치보다 **수평 확장 용이성(scalable)**이 핵심. 한국은행 자체 PoC에서 이 아키텍처로 **접수 15,000 TPS 이상·1건 0.014초 이내**가 확인됐다 — 단 **2센터·인메모리 무장에 전제의 부분 실증**이다(참고: TIPS 설계용량도 2,000 TPS·확장가능). 인메모리 장에 복원·순서 오류·3센터 확장 등 **미검증 급소는 차기 BMT로 실증**한다(6.4).
 2. **무중단 정의:** 무중단 배포가 기본, 자정 전후 짧은 계획점검(10~20분)은 예비 수단이자 정상 운영 → RTO 대상은 **비계획 장애**뿐(무복구 인계로 회복). 계승: ②(복원력)·⑤(거액 AA 시험대)·⑦(GSLB 단일접속)·⑩(야간 자동운영).

1. 과제 배경과 핵심 도전

1.1 왜 소액결제를 RTGS로 바꾸는가 — 디지털 뱅크런 차단

현재 우리나라의 소액 자금이체(인터넷·모바일뱅킹, 간편송금)는 **이연차액결제(DNS, Deferred Net Settlement)** 방식으로 처리된다. 쉽게 말해 **"고객 돈은 지금 즉시 옮겨주되, 은행끼리의 실제 정산은 다음 영업일 오전에 몰아서 한 번에"** 하는 구조다.

쉬운 비유: 친구끼리 밥값을 먼저 각자 내주고, 정산은 월말에 한 번에 몰아서 하는 것과 같다. 그 사이 "누가 누구에게 얼마를 빚지고 있는지"가 쌓인다.

이 "정산 시차" 동안 참가기관(은행) 사이에는 **외상(신용·유동성 리스크)**이 쌓인다. 평소에는 문제없지만, 한 은행이 갑자기 휘청이면 그 외상이 다른 기관으로 번질 수 있다. 특히 미국 실리콘밸리은행(SVB) 사태는 **모바일 시대의 예금 이탈(디지털 뱅크런)**이 몇 시간 만에 은행을 무너뜨릴 수 있는 속도를 보여줬다 — 이런 속도 앞에서는 "다음 영업일 정산까지"라는 시차 자체가 위험이 된다.

실시간총액결제(RTGS, Real-Time Gross Settlement)는 이 시차를 없앤다. 자금이체 건마다, 그 즉시, 은행 간 정산까지 완전히 끝낸다. 외상이 쌓일 틈이 없으니 신용리스크가 원천 제거된다. 한국은행은 이를 **2028년 전후 목표로 추진** 중이며, 야간·주말에도 대응 가능한 24시간 모니터링 체제를 함께 검토하고 있다.

1.2 또 다른 구축 필요성 — 현행 소액결제망의 단일 실패점(SPOF)

신용리스크 제거 외에, **현행 소액결제 인프라의 구조적 취약성**도 새 시스템 구축의 중요한 동인이다.

현행 전자금융공동망은 **단일 운영기관(금융결제원)**이 **중앙에서 중계·정산**하는 구조다. 모든 참가기관의 자금이체가 이 한 곳을 거친다. 이런 구조를 **단일 실패점(SPOF, Single Point of Failure)** 이라 한다.

단일 실패점(SPOF): 그 한 곳이 멈추면 전체가 멈추는 지점. 다리가 하나뿐인 섬에서 그 다리가 끊기면 섬 전체가 고립되는 것과 같다.

현행 구조의 한계는 운영 규칙에도 드러난다. 전자금융공동망 관련 규정은 장애가 나면 **"복구 후 이용하거나, 공동망을 거치지 않는 우회 거래로 안내"**하도록 정하고 있다. 즉 애초에 **"멈출 수 있다(비계획 장애도 복구 후 이용)"**를 전제로 한 설계이지, 무중단(비계획 장애에도 복구 없이 이어감)을 보장하는 설계가 아니다. 짧은 점검 시간대를 제외하면 사실상 24시간 가깝게 운영되고 있으나, **"항상 이용 가능"**이 제도적으로 보장되는 구조는 아니다.

여기서 말하는 "무중단"은 **0초도 멈추지 않는다는 뜻이 아니다**. 자정 전후의 짧은 **계획 점검창(10~20분, 필요 시에만 쓰는 예비 수단)**은 국제적으로도 "중단"과 구분되는 정상 운영이다(2.1절에서 상술). 문제는 **예고 없는 장애(비계획 중단)**다. 현행은 비계획 장애 시 "복구까지 기다리거나 우회"인데, 새 시스템은 이를 **복구 없이 즉시 이어받는(RTO≈0)** 수준으로 끌어올려야 한다.

소액결제가 이미 국민 일상의 필수 인프라(간편송금·급여·각종 자동이체)가 된 상황에서, **"멈출 수 있는 중앙 한 곳"**에 전 국민의 자금이체가 의존하는 것은 그 자체로 시스템 리스크다. 새로 구축할 소액 RTGS는 이 SPOF를 해소하여 **"한 곳이 죽어도 멈추지 않는" 다중화 구조**로 가야 한다. 이것이 본 보고서가 24/365 무중단 Active-Active를 핵심으로 다루는 두 번째 이유다.

정리하면 소액 RTGS 구축 필요성은 ① **신용리스크 제거(뱅크런 차단)**와 ② **단일 실패점 해소(무중단 복원력 확보)**라는 두 축으로 요약된다. ①이 "왜 RTGS인가"라면, ②는 "왜 (단일 중앙이 아닌) 무중단 다중 구조인가"의 답이다.

★ **오해 방지 — "취약하다면서 왜 병행 운영하나".** 본 보고서는 현행 공동망을 폐기 대상으로 보지 않는다. 신 시스템 가동 후에도 **현행 공동망과 상당기간 병행 운영**하는 것이 기본 방향이며, 이는 앞의 SPOF 해소 논리와 **모순되지 않고 오히려 그 이행 수단**이다. 이유는 두 가지다. 첫째, 신 시스템 초기 안정화 기간에 현행망이 **백업(fallback) 경로**가 되어 준다. 둘째, 반대로 현행망에 장애가 나도 신 시스템이 **우회로**가 된다. 즉 **"두 시스템이 서로의 대비책이 되는 이중 구조"** 자체가 **SPOF 해소의 실현**이다 — 단일 시스템(현행이든 신규든)에 전 국민 이체를 몰아넣지 않는 것이 핵심이다. 병행 운영의 구체 설계는 5.3에서 다룬다.

1.3 이 과제가 거액결제와 근본적으로 다른 이유 (역설)

회계결제시스템의 기존 거액결제(한은금융망 RTGS)와, 새로 만들 소액 RTGS는 **요구조건의 무게중심이 정반대**다. 이 점을 먼저 잡아야 이슈가 보인다.

비교 항목	거액결제 (현행)	소액 RTGS (신규)
가동 시간	평일 영업시간	24시간 · 365일 · 무중단
건당 금액	평균 약 251억원(매우 큼)	소액(건수가 폭발적)
하루 건수	한은금융망 약 2.3만 건	수백만~수천만 건(수백 배)
멈추면?	잠시 멈췄다 복구 가능	멈추는 순간이 곧 사고(밤·주말에도 뱅크런)
완결 단위	다자간 동시처리(여러 건을 한 덩어리로 묶어 처리)	건별 독립 완결
구축 방식	기존(2020년 차세대) 개선	신규 구축(백지 설계)

비유: 거액결제는 "낮에만 운행하고 고장 나면 잠시 세워도 되는 전세버스", 소액 RTGS는 "밤낮·주말 없이 멈추면 안 되고 한 대가 고장 나도 승객이 끊기면 안 되는 24시간 지하철"이다.

여기서 **역설**이 생긴다.

- **거액결제**는 여러 건을 한 덩어리로 묶어 동시에 끝내는 "다자간 동시처리"가 있어 **둘로 쪼개기(분산)가 매우 어렵다**. 그러나 영업시간만 돌아가므로 **무중단 부담은 작다**.
- **소액 RTGS**는 거래가 건별로 서로 독립이라 **여러 센터에서 나눠 처리(분산)하기 쉽다**. 그러나 24시간 멈추면 안 되므로 **무중단 부담이 최강이다**.

→ 즉 **거액은 "분산 어렵고 무중단 쉬움"**, **소액은 "분산 쉽고 무중단 어려움"**이다. 그래서 이 과제의 진짜 무게중심은 성능 자체가 아니라 **무중단 복원력**에 있다.

주의 — "분산이 쉽다"가 "계좌를 쪼개도 된다"는 뜻은 아니다. 거래가 건별 독립이라는 것은 *처리*를 여러 센터가 나눠 맡기 좋다는 뜻이지, *잔액 장부*를 센터별로 쪼개도 된다는 뜻이 아니다(왜 그런지는 2.1). 그래서 본 과제는 장부를 쪼개는 대신 **하나의 순서로 줄 세워 세 센터가 함께 재생**하는 방식을 택한다.

1.4 한국은행이 처리하는 것 — 참가기관 잔액

오해를 먼저 풀어둔다. 소액 RTGS가 가동되어도, **한국은행 원장이 기록하는 것은 개인(P2P)의 잔액이 아니라 참가기관(은행)의 잔액**이다. 개인 잔액은 각 은행이 자기 장부에서 관리한다.

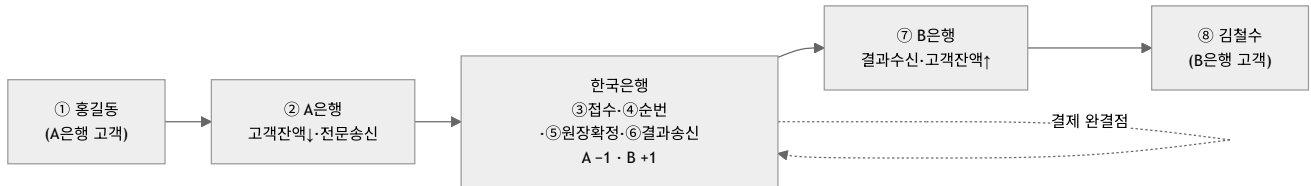
홍길동(A은행)이 김철수(B은행)에게 1만원을 보내면 — **한은 원장:** A은행 잔액 -1만원, B은행 잔액 +1만원 (한은가 하는 일) **A은행 장부:** 홍길동 -1만원 / **B은행 장부:** 김철수 +1만원 (각 은행이, 전문에 담긴 수취인 정보로)

소액 RTGS 가동 시 직접 참가기관은 이 용도의 **전용 결제계좌(원장)**를 한국은행에 새로 개설하게 된다. 거액결제가 "결제전용 당좌예금"을 별도로 둔 것과 같은 논리다. 다만 소액 RTGS는 거액(참가 약 134개)과 달리 **모든 기관이 직접 참가하지는 않는 구성이 유력하다** — 본 보고서는 "서버 접속 시중은행 약 20개 + 대형 핀테크 애그리게이터 2~3개"의 직접 참가를 작업 전제로 한다(상세는 2.5). 그 결과 한은 원장의

부하는 수십 개 수준의 전용계좌 잔액에, 하루 수백만~수천만 건의 증감이 집중되는 형태가 된다 — 계좌 줄이 거액보다 더 좁아 집중은 오히려 심하다. 이 부하 구조가 뒤(이슈 ③)에서 다룬 "핫 계좌" 문제의 뿌리다.

전체 송금 여정과 "완결점" — 어디서 결제가 끝나는가

한 건의 송금이 **고객 → 송금은행 → 한국은행(BOK) → 수취은행 → 고객**을 거치는 전체 여정에서, 본 시스템(BOK)의 역할과 책임 경계를 분명히 해둔다.



- **결제 완결(finality)은 오직 단계 ⑤(한은 원장 확정)에 선다.** 한은가 "A은행 -1만·B은행 +1만"을 **하나의 순번(원자적 이체)**으로 확정하는 순간, 은행 간 결제는 되돌릴 수 없이 끝난다. "A는 빠졌는데 B는 안 들어온" 중간 상태가 존재할 수 없다(저널 순차처리의 핵심 이점).
- **책임 경계:** 본 보고서의 3센터 아키텍처가 무중단·무이중지급을 보장하는 범위는 **단계 ③~⑥(한은 내부 + 참가기관 인터페이스)**이다. 고객↔은행 구간(단계 ①②⑦⑧)은 각 은행의 몫이다.
- **경계의 급소(단계 ⑥~⑦):** 한은는 확정했는데 수취은행이 결과전문을 못 받으면, 은행 간엔 결제됐으나 고객 반영이 지연된다. 이는 **결과전문의 역등 재송신 + 상시 대사(3.1)**로 흡수한다("한은 +1인데 B은행 미반영" 불일치를 대사가 포착). 이는 국제 표준 관행(한은 확정=은행간 완결, 고객 반영은 보장된 후속처리)과 동일하다.

1.5 이 과제가 풀어야 할 핵심 도전 (요약)

앞서 본 두 구축 동인 — **신용리스크 제거(1.1)**와 **단일 실패점 해소(1.2)** — 는 모두 결국 **"멈추지 않고, 정확하며, 충분히 빠른"** 시스템을 요구한다. 이 요구에서 도출되는 핵심 도전은 다음과 같다. 본 보고서는 이를 **기술 이슈 4개(2장)·운영 이슈 3개(3장)**로 나눠 각각 대응방안을 제시한다. 표의 ★ **항목 4개(접속·검증·평가·스택)**는 별도 이슈가 아니라 기술 이슈들을 뒷받침하는 **보완 절이며**, 2장에 함께 둔다.

구분	이슈	한 줄 요약
기술	① 무중단 복원력 (★최우선)	24/365·RTO≈0을 근거리 3센터로 어떻게 실현하나
기술	② 고성능·확장성	전국민·스파이크 부하를 견디며 유연 확장
기술	③ 원장 정합성·핫계좌	소수 전용계좌 갱신폭주·이중지급·순서변경 방지
기술	④ 전문 분산처리	폭주·중복·순서 꼬임 방지
기술	(★접속) 참가기관 접속	네 센터를 대표주소 하나로 — 장애가 나도 참가기관에겐 "안 보이게"(2.5)
기술	(★검증) 3센터 정합성	이중지급·split-brain 원천차단 + 순서오류 탐지·교정(2.3-부속)

구분	이슈	한 줄 요약
기술	(★평가) 신기술 적용가능성	인메모리·RDB·API·클라우드를 경로별로 가려 적용(2.6)
기술	(★스택) 기술 스택 구성	위 구조를 실제로 보장하는 계층별 솔루션(2.7)
운영	⑤ 마감 없는 무결성·대사	점검할 마감 시간이 없음
운영	⑥ 24/365 유동성 관리	야간·주말 결제유동성·참가기관 부담
운영	⑦ 무중단 운영·배포	멈추지 않고 고치기

2. 핵심 기술 이슈와 대응방안

2.1 이슈① 무중단 복원력 — 24/365와 "복구 없는 인계(RTO≈0)" ★최우선

이슈

중앙은행이 운영하는 소액 RTGS가 잠깐이라도 멈추면 평판에 치명적이다. 게다가 24시간 365일 돌아가므로 "장애 나면 야간에 복구하면 된다"는 여유가 없다. 무중단을 어떻게 보장하느냐가 이 과제 전체에서 가장 중요한 질문이다.

"무중단"의 정확한 정의 — 계획 점검은 허용, 비계획 장애엔 복구 없는 인계

먼저 "24/365 무중단"의 의미를 정확히 해야 한다. 완전한 무정지(0초도 멈추지 않음)는 현실적으로 불가능하며, 국제적으로도 그렇게 운영하지 않는다. 실제로는 두 가지를 엄격히 구분한다.

구분	성격	허용 여부	시간
계획 점검	예고된 시스템 점검·패치	✅ 허용 (예비 수단)	필요 시 자정 전후 10~20분, 최소 트래픽 시간대, 사전 공지
비계획 장애	예상치 못한 사고	❌ 복구 없는 인계	목표 RTO≈0(실질 무중단)

주요국 관행은 층이 나뉜다. **거액 계열(T2 등)**은 정산주기와 연동된 짧은 기술 점검창을 두지만, **즉시지급 계열(TIPS·FedNow)**은 중앙 인프라의 계획 중단 없이 **무중단 배포로 유지보수**하며 참가기관 측 점검창만 허용한다. 따라서 우리도 **무중단 배포(3.3)**를 기본으로 하되, 불가피한 대규모 변경에 대비해 **자정 전후 10~20분의 계획 점검창을 "예비 수단"으로 보유**한다 — 매일 상시 멈춘다는 뜻이 아니며, 사용 시에는 예고·최소 트래픽 시간대에 "계획된 점검"으로 구분해 공지한다.

진짜 목표는 **비계획 장애(사고) 시 사실상 멈춤 없이 이어가는 것**이다. 이를 기술 지표로 번역하면 두 가지다.

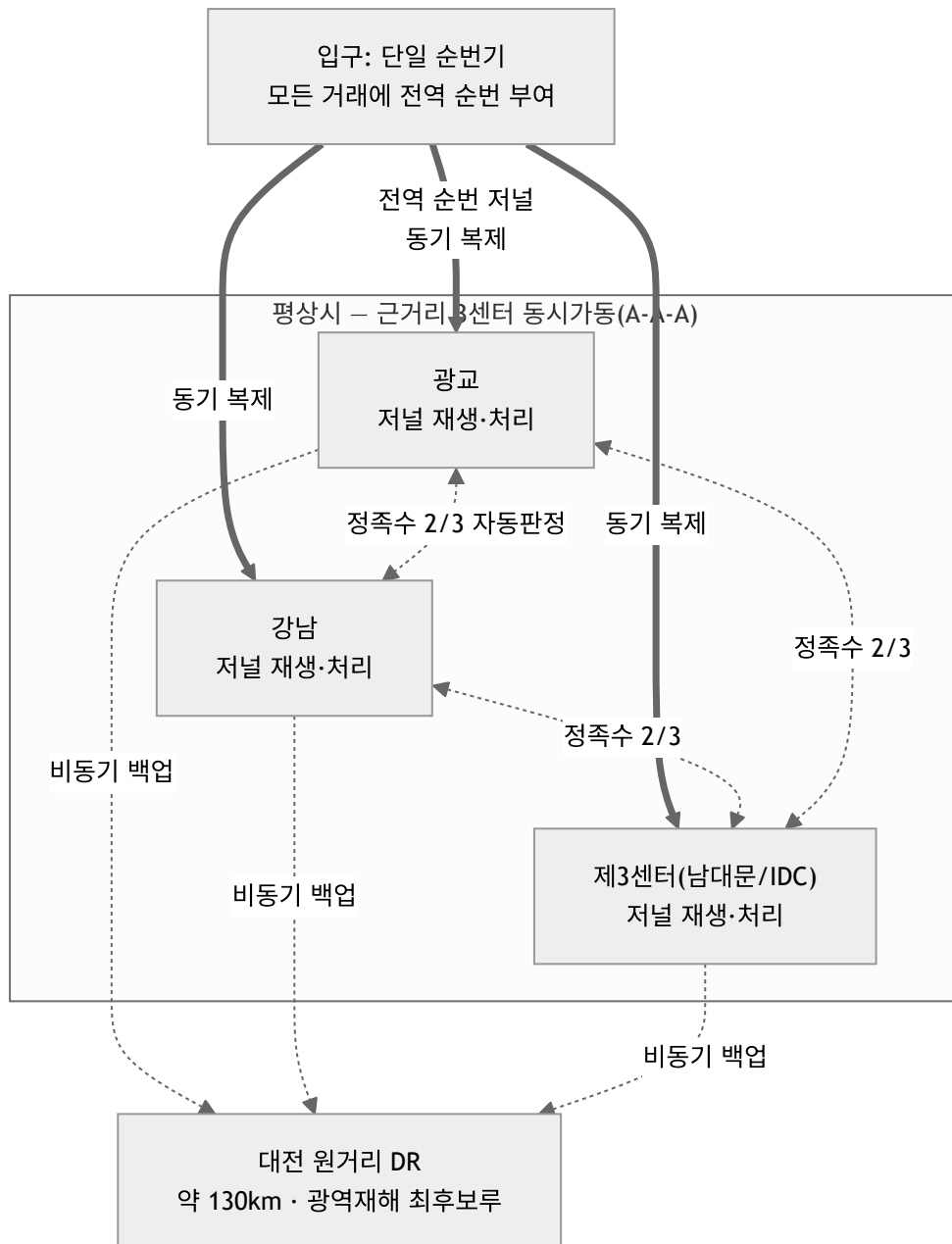
지표	뜻	본 과제 목표
RTO(복구 목표시간)	비계획 장애 후 서비스 재개까지	≈0 — 복구 없이 즉시 인계
RPO(복구 목표시점)	잃어도 되는 데이터 범위	0 (결제는 단 1건도 못 잃음)

왜 "5분"이 아니라 "0"인가. 기존에는 복구목표를 "5분 이내"로 잡았으나, "복구 시간이 존재한다"는 것 자체가 "꺼진 무언가를 다시 켜다"는 뜻이며, 예고 없는 사고에서 몇 분의 공백은 결코 안전하지 않다(중앙은행 결제망이 새벽에 몇 분만 멈춰도 그 자체가 사고다). 따라서 목표를 "복구할 것이 없는 구조(RTO≈0)"로 올리고, "5분"은 달성 목표가 아니라 "이 선을 넘으면 중대사고로 간주하는 절대 상한선(레드라인)"으로 재정의한다. 이는 유럽 TIPS가 3센터 동시가동으로 복구목표시간을 사실상 0(zero)으로 끌어올린 것과 같은 방향이다. 본 과제는 국제 기준을 넘어서려는 것이 아니라, TIPS의 검증된 모범을 우리 여건에 맞게 쫓는다. 가용성 목표 수치(예: TIPS의 99.9% 이상)는 처리시간 목표와 함께 局간 협의로 확정한다(6.1-9).

대응방안 — 근거리 3센터 Active-Active-Active + 저널 순차처리

무중단의 근본 구조로 근거리 3센터를 모두 동시에 가동(Active-Active-Active)하고, 세 센터가 하나의 거래 명단(저널)을 같은 순서로 나눠 처리하는 방식을 채택한다. (왜 디스크 통째 복제가 아니라 "저널" 복제인지 — 스토리지 복제의 함정은 3.1에서 정리한다.)

왜 2센터가 아니라 3센터인가 — "심판이 있어야 무승부가 안 난다". 센터가 둘뿐이면, 둘 사이 통신이 끊겼을 때 누가 살아있는 진짜인지 판정할 수 없다. 두 센터가 서로 "상대가 죽었다"고 오인하면, 양쪽이 동시에 같은 계좌를 건드려 이중지급이 난다(split-brain, 2.3-부속에서 상술). 이를 막으려면 홀수(3표)로 과반을 정하는 심판 구조가 필요하다. 세 센터가 모두 깨어 있으면, 하나가 죽어도 나머지 둘이 곧 과반(2/3)이므로 "누가 진짜인지"가 자동으로 정해지고, 살아남은 둘은 이미 같은 최신 상태로 돌고 있어 복구 없이 즉시 잇는다.



이 방식의 핵심 — "번호표 발급기" 비유. 세 센터가 담당 은행을 나눠 맡는 대신, **입구에서 모든 거래에 전국 통일 번호표(전역 순번)를 매긴다.** 그 번호표 명단(저널)을 세 센터가 똑같이 받아 같은 순서로 처리한다. 순서가 번호표에 이미 확정돼 있으니 센터끼리 "누가 먼저 할지" 협의할 일이 없고, 같은 명단을 같은 순서로 처리하면 어느 센터든 결과가 반드시 같아진다. (개인 간 송금은 모든 은행이 얹혀 "담당 나누기"로는 조울 비용이 크지만, 번호표 방식은 그 문제 자체가 없다.) 이 방식이 실제로 어떻게 이중지급·순서변경을 원천 차단하는지는 **2.3-부속에서 정면 검증**한다.

이 구조가 무중단(RTO≈0)을 푸는 원리는 세 가지다.

(1) 전환이 아니라 인계 — 그래서 즉시다. 세 센터가 같은 저널을 **동시에 재생**하고 있으므로 잔액 상태가 항상 일치한다. 한 센터가 죽어도 나머지 둘은 **새로 켜거나 데이터를 옮겨올 필요 없이 이미 같은 상태 그대로** 처리를 이어간다. 재기동·캐시 준비가 없으므로 복구 공백이 사실상 없다(꺼진 것을 켜는 "페일오버"와 결정적으로 다른 점이다).

(2) 판단은 자동 — 몇 분 안에 사람이 못 깨므로. 새벽 3시 일요일에 당직자가 깨어나 전환 명령을 내릴 시간은 없다. 따라서 거액결제 복원력(과제 ②)에서 정한 **"결정은 사람, 실행은 자동" 원칙이 여기서는 "결정조차 자동"으로 한 발 더 나아간다.** 세 센터가 자동 투표(정족수 2/3)로 "누가 살아있나"를 정하고, 응답 없는 센터는 펜싱(fencing, 강제 차단)하여 반쯤 살아난 센터가 같은 계좌를 또 건드리는 일(이중쓰기)을 막는다. 이 펜싱·정족수 장치는 과제 ②에서 이미 설계한 것을 계승·강화한 것이다.

(3) 대전은 광역재해 최후보루. 대전은 약 130km로 동기복제가 불가능한 거리다. 따라서 근거리 3센터의 동시재생에는 참여하지 않고, 비동기 백업만 담당한다. 수도권 전체가 재해를 입어 근거리 3센터를 동시에 잃는 최악의 경우에만, 약간의 데이터 손실(RPO>0)을 감수하고 최후 보루로 가동한다. 이때의 "손실"이 **완결 선언된 결제의 소멸을 뜻하지는 않는다** — 이미 참가기관에 응답이 나간 확정분 중 대전에 못 미친 부분(gap)은 참가기관이 보유한 응답 전문과의 대사로 재구성해 재적용한다(과제 ②의 gap 복구 계승). 이 복원 절차는 결제 완결성 법제(6.1-14)에 규정으로 함께 못박아 둔다.

제3센터를 어디에 둘 것인가 — 남대문 본점 우선

근거리 3센터가 되려면 **광고·강남에 더해 세 번째 근거리 동기센터**가 필요하다. 후보는 다음 순서로 검토한다.

순위	제3 근거리 센터	평가
1	남대문 본점 자체 구축	한국은행 소유 건물 → 폐쇄망·물리보안·통제권 최상, 임차료 없음. 단 전산센터급 공간·전력·냉방 조성 필요
2	수도권 상용 IDC 임차	신속 확보 가능하나 결제 원장을 외부 시설에 두는 보안·위탁 부담, 임차료 발생
(공통)	+ 대전 원거리 DR	수도권 광역재해(3센터 동시 상실) 최후보루 — 어느 안이든 필수

남대문 본점은 강남과 약 10km, 광고와 약 30여 km로 **세 구간 모두 동기복제 가능 거리(50km 이내)에 든다**(세 구간 실측 왕복지연은 확인 필요 — 6장). 결제 원장이 **한국은행 통제 구역을 벗어나지 않는다는 점**에서 폐쇄망 운영 원칙(2.6절 클라우드 평가 참조)에 가장 부합한다.

※ 본 근거리 제3센터(남대문 본점 또는 수도권 IDC)는 소액 RTGS 전용 신규 구축에 한한다. 회계결제시스템(거액) 3센터 구성(광고·강남·대전)과는 **별개**이며, 물리 인프라 공유 여부는 유관 부서 간 **별도 협의 사항**이다.

근거리 3센터의 역설 — 그래서 대전 원거리 DR은 여전히 필수

근거리 3센터는 복구 없는 인계(RTO≈0)를 얻는 대신, 세 센터가 **같은 수도권의 전력·통신망을 공유**한다는 약점이 있다. 지진·광역정전·통신대란 같은 **수도권 광역재해 시 세 센터가 동시에 멈출 수 있다.** 따라서 **원거리 대전 DR**(약 130km, 비동기 복제)을 최후보루로 둔다. 이 경우에만 약간의 데이터 손실(RPO>0)과 분 단위 복구를 감수한다. **"근거리 3센터(RTO≈0) + 원거리 1센터(광역재해 대비)"의 2계층**이 완성형이며, 이는 TIPS 등 해외 사례의 2계층 복원력 구조와 동일하다.

정직한 트레이드오프 — RTO≈0은 공짜가 아니다. 이 구조는 근거리 3센터에 원거리 DR까지 **실질 4개 물리센터**를 요구한다(제3센터가 신규 구축이면 그 부담이 특히 크다). 즉 **"복구 없는 무중단"의 대가로 구축·운영 비용과 복잡도가 크게 늘어난다.** 그러나 소액 RTGS는 24/365 국민 필수 인프라이자 중앙은행 평판이 걸린 시스템이므로, 이 비용은 **가용성을 위해 지불하는 정당한 값**으로 판단한다. 다만 규모가 큰 만큼 제3센터 확보 방식(자체구축/임차)은 비용·기간을 함께 저울질해 결정한다(6장).

참고 — 샤딩(계좌 소유 분담)은 왜 본안이 아닌가

한때 "거래가 건별 독립이니 계좌를 센터별로 나눠 맡기면(샤딩) 된다"는 방안을 검토했다. 그러나 소액 RTGS의 주력인 개인 간 송금(P2P)은 **모든 은행이 모든 은행과 얽혀**, 담당 센터를 넘나드는 거래(교차거래)가 구조적으로 많다. 이 경우 두 센터를 걸치는 무거운 조율(분산 트랜잭션)이 강제되어 오히려 복잡하고 느려진다. 저널 순차처리는 애초에 하나의 순번으로 줄 세우므로 이 문제가 발생하지 않는다. **따라서 저널 순차처리를 본안으로 하며, 샤딩은 교차거래 비율이 낮게 측정될 경우의 부하분산 최적화 옵션으로만 남긴다**(교차거래 비율은 6장 확인필요).

2.2 이슈② 고성능·확장성 — 목표 TPS 산정

이슈

소액 RTGS는 전 국민이 이용한다. 평소 부하도 크지만, **뱅크런·재난지원금·명절·티켓팅처럼 한순간에 트래픽이 폭주(스파이크)**한다. "평소 평균"이 아니라 **"최악의 동시 몰림"**을 견디는 용량이어야 한다. 또한 이용 규모가 해마다 늘어날 것이므로 **유연하게 확장 가능한** 구조여야 한다.

대응방안 — 현행 피크를 기준선으로, 확장성(scalable)을 핵심으로

목표 설정의 출발점은 **현행 전자금융공동망의 실측 최대 피크**다. 이는 **초당 약 2,000건(TPS)**을 넘지 않는 수준이다. 이것이 "최소한 이만큼은 처리해야 한다"는 **기준선**이 된다.

그러나 **"현행 피크가 2천 미만이니 목표도 2천이면 된다"**는 결론은 위험하다. RTGS 전환은 부하의 성격 자체를 바꾸기 때문이다.

변화 요인	부하에 미치는 영향
이연 일괄 → 건별 즉시 처리	거래가 발생 즉시 시스템에 도달(완충 없음)
영업시간 → 24/365 가동	야간·주말 이용 신규 발생
미래 이용 성장	간편송금·즉시지급 수요 지속 증가
이벤트 스파이크	재난지원금·명절·뱅크런 시 순간 폭주

→ 따라서 목표는 고정된 숫자를 못 박는 것이 아니라, **현행 피크(약 2,000 TPS)를 기준선으로 삼되 그 이상으로 유연하게 확장 가능하게(scalable) 짓는 것**이다. 이용 규모가 늘면 **처리기(노드)**를 추가하는 것만으로 **처리량이 비례해 늘어나는 수평 확장(scale-out)** 구조를 원칙으로 한다. 고정 용량으로 지었다가 한계에 부딪혀 시스템을 통째로 교체하는 방식(수직 확장)은 24/365 무중단 시스템에 부적합하다.

단, 정직하게 구분할 것이 있다 — 수평 확장이 그대로 통하는 곳은 입구·검증·조회 등 **병렬 구간**이다. 전역 순번을 매기는 **직렬 코어(순번기)**는 노드를 늘려도 **"한 줄"**이라는 본질이 바뀌지 않으므로, 증설이 아니라 **한 건당 처리시간 단축(메모리 처리·경량 명령문, 2.7)과 상한 실측(6.4)**으로 관리한다(2.3-부속 전제①).

실증으로 확인된 확장 여력(단, 범위 한계 명시). 국내 자체 PoC에서 본 보고서와 같은 계층 구조 (이벤트 브로커·인메모리·원장 DB)로 **접수 처리 15,000 TPS 이상·1건 응답 0.014초 이내**가 달성됐다. 즉 목표 상한을 현행 피크(2,000)에 가둘 이유가 없으며, 그 수 배까지 확장 가능성이 확인됐다. **다만 이 수치는 ① 한은-참가기관 구간 한정(고객단 end-to-end 아님) ② 인메모리 무장애 전제 ③ 2센터 기준 ④ 응답·완결 규율(과반 확정 후 응답, 2.3-부속) 미적용의 이상적 부하시험 결과다.** 실거래의 보안·암복호화·예외처리를 얹으면 낮아지므로 **"실증 가능치 ≠ 실제 필요량"**이며, 필요량은 이용규모로 결정한다.

참고 — 유럽 TIPS도 설계용량 2,000 TPS이며 확장 가능하다. 즉 TIPS는 처음부터 낮은 고정치가 아니라 **"기준 용량 + 확장"** 사상으로 설계됐고, 이는 우리의 scalable 원칙과 같은 방향이다. 핵심은 절대 수치가 아니라 **"필요한 만큼 늘릴 수 있는 확장성"**에 있다.

(주: 앞선 검토 단계에서 간편지급(카드·페이 결제) 건수까지 합산해 7,500 TPS 이상으로 산정한 바 있으나, 간편지급 상당수는 전자금융공동망을 직접 경유하지 않고 카드망 등을 통하므로 과대계상이었다. RTGS 전환 대상에 부합하는 현행 실측 피크는 약 2,000 TPS 미만이며, 이를 기준선으로 정정한다.)

2.3 이슈③ 원장 정합성·핫 계좌 — 이중지급 방지

이슈

앞서 본 대로 한은 원장의 부하는 **수십 개의 전용계좌 줄에 집중**된다(참가 구성 전제는 1.4-2.5). 계좌 수는 적은데 갱신은 엄청나게 많고, 특히 거래가 큰 은행(대형은행)과 애그리게이터의 계좌에 갱신이 몰린다(핫 계좌). 여기서 가장 위험한 사고가 **이중지급**이다. A은행 잔액이 100만원인데 두 센터가 동시에 80만원씩 출금을 승인하면(둘 다 "잔액 충분"으로 읽음) 합계 160만원이 빠져 **돈이 허공에서 생긴다**. 이는 중앙은행이 절대 허용할 수 없는 사고다.

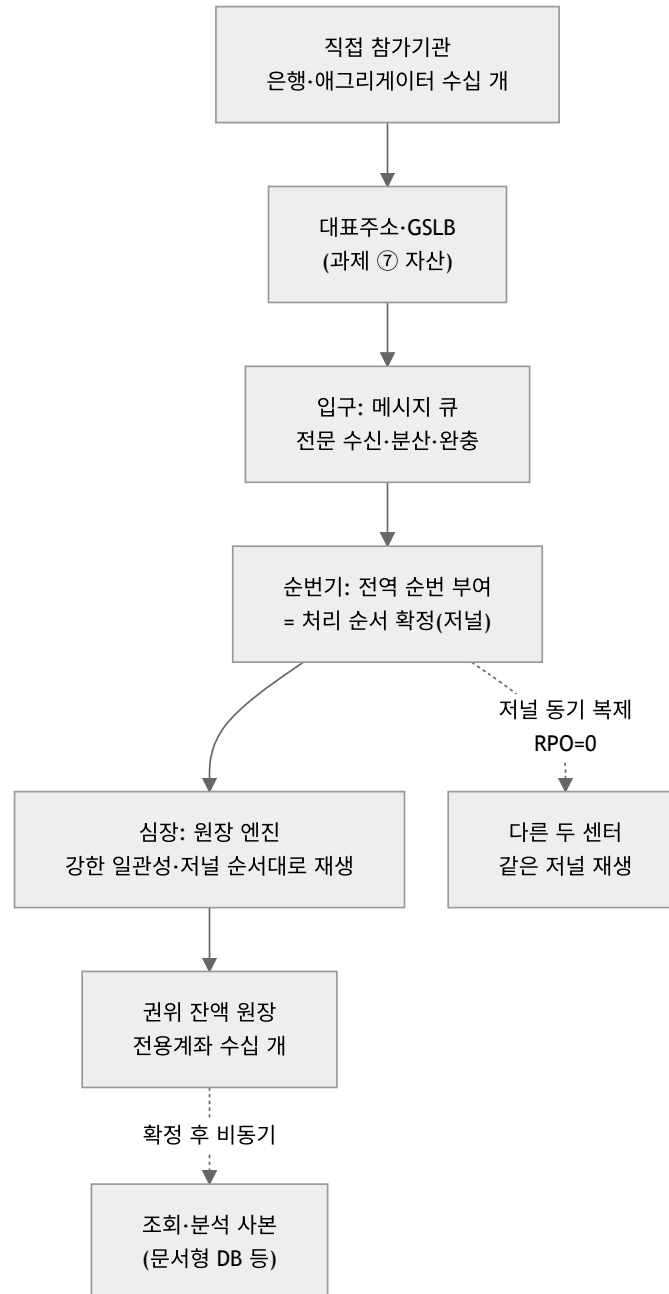
대응방안 — 전역 단일 순번 + 저널 재생 + 강한 일관성

해법은 이미 이슈①의 **저널 순번부여** 구조에 들어 있다. 모든 거래가 하나의 전역 순번으로 줄 세워지므로, 1번이 잔액을 깎으면 2번은 그 결과를 본 뒤 처리된다 — **같은 계좌를 두 곳이 "동시에" 건드리는 상황 자체가 없다**. 세 센터가 같은 순서로 재생하니 어디서 보든 잔액이 같다. (이중지급·순서변경이 왜 구조적으로 불가능한지는 2.3-부속에서 정면 검증한다.)

덤 — 핫 계좌가 별도 난제가 되지 않는다. 계좌를 센터별로 쪼개는 방식이었다면 대형 은행 계좌가 병목이 됐겠지만, 저널 순차처리는 **어차피 모든 거래를 순번 순서대로 처리**하므로 특정 계좌에 몰린

아니든 처리 방식이 같다. 관건은 그 한 줄(순번기)의 속도이며, 코어를 메모리에서 처리해 이를 최대한 빠르게 흘린다(2.7).

남은 핵심은 **시스템 도구를 역할에 맞게 배치**하는 것이다. 결제 원장의 잔액 확정만큼은 "**강한 일관성 (strong consistency)**" — "항상 정확한 최신 잔액을 보장하고, 의심스러우면 차라리 멈추는" 엄격한 방식 — 을 쓴다. 아래 표는 **원장을 중심으로 한 3역할 분리**를 보이며, 시스템 전체의 5계층 스택은 2.7에서 다룬다.



역할	적합 도구	이유
전문 수신·분산·완충(입구)	메시지 큐	폭주를 완충하고 처리기로 분배
잔액 확정(심장 = 원장)	강한 일관성 엔진	이중지급 방지엔 "단일 순번 + 강한 일관성" 필수

역할	적합 도구	이유
조회·분석·이력(사본)	문서형 DB 등	확정된 결과의 읽기 전용 사본

중요한 설계 경고: 메시지 큐나 문서형 DB는 흔히 "**최종적 일관성(eventual consistency)**" — "지금은 두 곳이 달라도 조금 있으면 같아진다"는 방식 — 을 기본으로 한다. 장바구니·피드에는 훌륭하지만 **결제 잔액에는 치명적**이다(옛 잔액 읽기·순서 뒤바뀔·중복 처리 → 이중지급). 따라서 이런 도구는 **입구와 사본에만 쓰고, 잔액 확정(원장)에는 쓰지 않는다**.

2.3-부속 3센터 정합성의 기술적 검증 — 이중지급은 왜 불가능하고 순서오류는 어떻게 잡는가 (★검증)

"세 센터가 실시간으로 같은 상태를 유지한다"는 주장은 결제 시스템에서 반드시 **정면 검증**되어야 한다. 네 가지 위험을 하나씩 논증하되, "**구조가 막는 것**"과 "**장치로 잡는 것**"을 구분한다(완벽을 가정하지 않는다).

위험 1 — 순서 변경(센터마다 처리 순서가 달라짐): 설계로 보장 + 탐지·교정 장치 병행 모든 거래는 입구의 **단일 순번기(sequencer)**에서 전역 순번을 부여받는다. 이 순번이 곧 처리 순서이며, 세 센터는 **순번이 박힌 저널(명단)을 복제받아 번호 순서대로 재생**한다. 같은 명단을 같은 순서로 처리하면 어느 기계든 반드시 같은 결과가 나온다(**결정론적 재생**).

다만 여기서 "**순번 부여**"와 "**순번대로 적용**"은 다른 문제임을 정직하게 짚어야 한다. 순번기가 번호를 정확히 매겨도, 세 센터가 병렬로 저널을 받아 재생하는 과정에서 **네트워크 재정렬·버퍼·비동기 I/O로 적용 순서가 드물게 어긋날 수 있다**(실제 국내 PoC에서도 순서 오류가 드물게 관찰됐다). 따라서 "순서변경은 원천 불가능"이라고 단언하지 않고, **순서를 보장하도록 설계하되 어긋남을 탐지·교정하는 장치를 병행**한다.

- 각 센터가 저널 적용 시 **순번 연속성 검사**(gap = 빠진 번호 / 역전 = 순서 뒤바뀔 탐지)
- 이상 발견 시 **제자리 순번이 올 때까지 보류(pending) 후 순서대로 재적용** — 저널이 원본이므로 재생 가능
- 잔류 불일치는 **상시 대사(3.1)**가 세 센터를 대조해 포착

비유: 세 회계사에게 같은 전표를 같은 번호 순서로 나눠주되, 혹시 전표가 뒤섞여 도착하면 **번호를 확인해 제 순서에 끼워 넣은 뒤 계산**한다. 이 "번호 확인 후 정렬" 절차가 순서 오류를 흡수한다.

★ 이 처방은 모의 시뮬레이션으로 **정량 확인됐다(부록 A)**. 순서 오류를 주입했을 때, 교정 장치가 없으면 의존 거래(입금→그 돈으로 출금)에서 잔액부족 **오거절이 1,300여 건** 발생했으나, **탐지·교정 장치를 켜면 정답과 동일(오거절 최소)**으로 수렴했다.

응답·완결 규율 — 판정의 권위는 "과반 확정"에만 있다. 순서가 어긋난 채 재생하면 판정(승인/거절)도 어긋날 수 있으므로, 참가기관에 나가는 결과 응답은 ① 해당 순번까지 **빠짐·역전 없이 연속 적용**을 마치고 ② **과반(2/3) 센터가 같은 순번까지 확정했음**이 확인된 뒤에만 송신한다. 1.4의 완결점("한은 원장 확정")의 정밀 정의가 바로 이것이다 — **완결 = 과반 센터가 해당 순번 적용을 확정**한 시점이며, 어느 한 센터의 단독 판정은 대외 효력을 갖지 않는다. 이 규율이 지켜지는 한 순서 오류는 **응답 지연**으로 나타날 뿐 **잘못된 응답이 밖으로 나가지 않는다**(부록 A S4의 오거절 1,300여 건은 이 규율 없이 재생했을 때의 피해를 보인 것이다).

위험 2 — 이중지급(두 센터가 같은 잔액을 동시에 깎음): 불가능 이중지급은 두 곳이 같은 잔액을 "동시에" 읽고 각자 깎을 때 난다. 그런데 잔액을 바꾸는 거래가 **모두 하나의 순번 줄에 세워지므로**, 100번 거래가 잔액을 깎으면 101번은 그 결과를 본 뒤에 처리된다. **"동시에"라는 상황 자체가 없다.** 설령 같은 송금이 중복으로 두 번 들어와도, **멱등성(idempotency)** 검사로 "이미 처리된 거래번호"임을 확인해 두 번째를 무시한다. (이 "불가능"은 위의 응답·완결 규율과 멱등성이 지켜짐을 전제로 한 구조적 차단이다.)

위험 3 — split-brain(통신 단절 시 양쪽이 각자 "내가 진짜"라 우깁): 불가능 세 센터 사이 통신이 갈라져도, **과반(2표)을 켜 쪽만 계속 처리하고 1표만 남아 고립된 쪽은 스스로 멈춘다**(정족수 규칙). 소수파는 과반이 아니므로 "내가 진짜"라 우길 수 없다. 혹시 고립된 센터가 오작동으로 계속 처리를 시도해도 **펜싱(강제 차단)**이 그 쓰기를 물리적으로 막는다. **2센터라면 1:1로 갈려 누구도 과반이 아니라 판정 불능이지만, 3센터는 반드시 2:1로 갈려 과반이 정해진다 — 이래서 홀수 3센터라야 한다.**

위험 4 — 조회 시점 불일치(같은 순간 세 센터 잔액이 다르게 보임): 발생 가능하나 무해 + 규정 조회는 별도 규율 세 센터가 같은 저널을 재생하지만 **재생 진도가 완벽히 동시**는 아니다. 광고가 100번까지 적용했을 때 강남이 99번까지일 수 있다(수 ms 차이). 이 찰나에 세 센터에 잔액을 각각 물으면 **답이 순간적으로 다를 수 있다.** 그러나 이는 "틀린 값"이 아니라 **"약간 옛 시점의 정확한 값"**이다 — 순번 순서로만 나아가므로 미래를 앞질러 본 값은 절대 나오지 않으며, 재생을 마치면 세 센터 최종 잔액은 **반드시 같다.** 결정적으로, ****잔액을 *바꾸는* 것은 하나의 순번 줄로 직렬화되므로 이 조회 시차는 결제 정합성·이중지급에 전혀 영향이 없다.****

- **운영 조회**(참가기관 실시간 잔액): 아무 센터에서나 응답하되, 한 참가기관의 연속 조회가 거꾸로 보이지 않도록 두 가지 규율을 적용한다 — **단조 읽기(monotonic read)** = 한 번 본 잔액보다 더 과거 값으로 되돌아가 보이지 않게, **자기 쓴 값 읽기(read-your-writes)** = 방금 내가 보낸 이체는 반드시 반영돼 보이게. 조회 부하는 조회 전용 사본(2.3 표의 "사본")으로 분산한다.
- **★ 규정 조회**(지급준비금 판정·마감 잔액·대사 등 "확정값"이 필요한 업무):

먼저 쉬운 원리: 같은 책을 같은 페이지까지 읽으면 세 사람의 내용이 똑같다. 마찬가지로 세 센터가 **"몇 번 순번까지"만 똑같이 맞추면** 잔액이 반드시 같아진다. 그래서 규정값은 "어느 센터에서 보느냐"가 아니라 **"몇 번 순번 기준이냐"**로 정하면 된다.

이 원리를 그대로 쓴다. **별도의 "공통 원장 한 권"을 두지 않는다**(그 자체가 SPOF가 된다). 대신 **"기준 순번(sequence point) — 몇 번 거래까지 반영한 상태인지 못박는 기준점"**으로 값을 고정한다. 예컨대 "○시 마감 = 순번 N번까지 적용된 상태"로 정하면, 어느 센터에서 읽든 값이 같다(단, 빠짐·역전 없는 정상 재생을 마친 센터만 응답 — 검사 미통과 센터는 규정 조회에 응답하지 않는다). 운영·감사 편의로 **1차 기준 센터**를 둘 수 있으나, 그 센터가 죽으면 **정족수 규칙으로 다른 센터가 기준을 이어받는다**(순번이 같으니 값도 그대로 → SPOF 아님). TIPS-FedNow가 지준·마감 잔액을 다루는 방식과 정합한다.

정직한 검증 — 이 논리의 전제와 대가(공짜가 아니다).

전제 / 한계	내용	대응
① 단일 순번기 병목	순서를 한 줄로 세우니 순번기가 처리량 상한이자 새 단일점	순번기 자체도 3센터 이중화(리더가 죽으면 정족수 합의로 새 리더). 코어는 메모리 처리로 가속 → 한계는 PoC 실측(6장)

전제 / 한계	내용	대응
② 동기 대기 지연	세 센터 과반이 저널을 받았음을 확인해야 확정 → 매 거래에 센터 간 왕복 지연 가산	근거리(20~35km)라 왕복 수 ms. 그래서 거리가 생명 — 세 센터가 동기거리 내려야 성립
③ 결정론 재생의 함정	처리 로직에 시각·난수 등 "센터마다 다를 수 있는 값"이 끼면 재생 결과가 어긋남	그런 값은 순번기가 저널에 미리 박아 배포(모든 센터가 같은 값 사용) — 설계 규율 필요
④ 순번기 앞단 취약구간	순번을 받기 "직전"의 거래는 아직 어느 저널에도 없음 → 그 순간 입구 장애 시 유실 가능	입구 메시지 큐 다중화·재전송 + 참가기관 재송신(먹등성이 중복 흡수)
⑤ 인메모리 코어 장애	잔액을 메모리에서 연산하므로, 노드가 죽는 순간 메모리에만 있고 확정 전인 거래 가 유실될 수 있음	★ 선(先)저널 규율(write-ahead) : 메모리 연산 전에 저널에 순번을 먼저 확정 한다. 그래야 노드가 죽어도 살아있는 센터가 그 저널로 재생해 무손실 승계(부록 A S2에서 확인). *국내 PoC는 인메모리 무장애를 전제해 이 지점은 미검증 → BMT 필수*

예상 반론 — "SPOF를 없앴다더니, 순번기라는 새 SPOF를 만드는 것 아닌가?" 타당한 지적이며 정면으로 답한다. 본 과제가 해소하려는 SPOF(1.2)는 **"멈추면 복구까지 전체가 서는 단일 운영 지점"**이다. 순번기는 다르다 — **순번기 자체를 세 센터에 이중화**하여, 순번을 발급하는 리더가 죽으면 정족수 합의로 남은 센터가 즉시 새 리더가 된다(끄고 켜는 복구가 아니라 무중단 승계). 즉 순번기는 "기능상 하나의 순서를 만들되, 물리적으로는 단일점이 아닌" 구조다. TIPS 등 해외 즉시지급 시스템도 코어 순서 부여를 이처럼 다중 노드 합의로 이중화하는 것으로 알려져 있다. **"논리적 단일 순서 ≠ 물리적 단일 장애점"** — 이 구분이 핵심이다. 물론 승계가 공짜는 아니다 — 리더 재선출(정족수 재합의)에는 짧은 시간이 걸리고 그동안 신규 순번 발급이 잠시 멈춘다. 다만 진행 중 거래는 입구 큐가 보관했다가 이어 처리하므로 **유실 없이 지연만 발생**하며, 이 승계 공백이 RTO≈0의 "≈"가 감당하는 범위다(실제 길이는 BMT로 실측 — 6.4).

검증 결론: 이중지급·split-brain은 구조 자체가 원천 차단(단일 순번·정족수·펜싱)하고, **순서 오류는 구조가 최소화**하되 탐지·교정 장치가 흡수한다. 그 대가로 ①순번기 병목·②동기 지연이 생기며, 이는 **근거리 배치(거리 실측)와 순번기 처리량 검증(PoC)**으로 관리한다. 이 구조의 각 요소는 **모의 시뮬레이션(부록 A)에서 코드로 검증**됐고, 국내 PoC에서도 **2센터 기준 데이터 정합성·자동복구가 확인**됐다(단, PoC는 한은-참가기관 구간·인메모리 무장애 전제·2센터라는 범위 한계가 있으므로 4장·6장 참조). 근거리 3센터 확장·인메모리 장애 복원·순서 오류율은 다음 실증(BMT) 단계의 과제다. 아울러 "원천 차단"은 정족수·펜싱·선저널 같은 장치의 **올바른 구현**을 전제한다 — 같은 소프트웨어 결함이 세 센터에 똑같이 복제되는 **상관 장애**는 구조가 막지 못하므로, 상시 대사·오염 탐지(3.1)와 배포 단계 검증(3.3)이 그 방어선이다.

2.4 이슈④ 전문 분산처리 — 폭주·중복·순서

이슈

참가기관·개인이 보내는 송금 지시(전문, ISO 20022 표준 메시지)가 한 입구에 몰리면 **병목·정체**가 생긴다. 또한 같은 송금이 두 번 들어오거나(중복), 입금보다 출금이 먼저 처리되는(순서 꼬임) 위험이 있다.

대응방안 — 메시지 큐 입구 + 순번기 + 멍등성

전문 수신·분산은 **입구(메시지 큐)**가 담당한다. 폭주가 와도 큐가 완충하고, 여러 처리기가 큐에서 꺼내 형식 검증·중복 제거 등 주변 작업을 나눠 처리한다. (해외 즉시지급 시스템의 공개된 구현 사례에서도 이 역할에 메시지 큐 기술이 쓰인다.)

순서 꼬임은 입구 바로 뒤의 **순번기(sequencer)**가 푼다. 주변 작업을 마친 거래는 순번기에서 전역 순번을 받고, 그 순서가 곧 원장 처리 순서가 된다(2.3). 즉 **"여러 줄로 받아 완충·검증(병렬)하되, 잔액을 바꾸는 순간은 한 줄로 세운다(순차)."**

중복은 **멍등성(idempotency)**으로 푼다.

멍등성: 같은 지시를 몇 번 보내도 결과는 딱 한 번만 반영되는 성질. 엘리베이터 버튼을 여러 번 눌러도 엘리베이터는 한 번만 오는 것과 같다.

각 송금에 고유 번호를 붙여, 같은 번호가 또 들어오면 "이미 처리됨"으로 무시한다. 이 개념은 과제 ②·⑦에서 이미 다룬 것을 그대로 적용한다.

경계에서의 정합성 — 다른 시스템과의 접점. 소액 RTGS는 고립된 섬이 아니라 한은금융망(거액)·타 결제시스템과 연결된다. 이 **경계를 넘는 거래**에서도 "한 번만, 정확히"가 지켜져야 한다. 원칙은 동일하다 — 접점마다 **고유 거래번호와 멍등성**으로 중복을 흡수하고, 필요한 경우 **결과 확정 통지(완결 확인)**를 주고받아 양쪽 장부의 어긋남을 막는다. 구체 연계 방식은 대상 시스템별로 별도 설계하되, 본 과제의 저널·멍등성 원칙이 그 토대가 된다.

2.5 참가기관 접속 구조 — 대표주소 하나로 네 센터를 잇는다 (★접속)

참가 구성 전제 — 거액과 다른 "좁은 직접 참가"

소액 RTGS는 거액(한은금융망 참가 약 134개)과 달리 **모든 기관이 직접 참가하지는 않는** 구성이 유력하다. 본 보고서는 다음을 작업 전제로 한다(참가 제도 자체는 미확정 — 6장).

구분	구성(전제)	접속 형태
직접 참가	서버 접속 시중은행 약 20개	자체 서버 상시 접속, 전용계좌 보유
직접 참가	대형 핀테크 애그리게이터 2~3개(간편송금 플랫폼 등)	자체 서버 접속, 전용계좌 보유 — 트래픽 비중이 크고 변동성 최대
간접 참가	그 밖의 기관	직접 참가기관(은행·애그리게이터)을 경유해 결제

애그리게이터(aggregator): 다수 이용자·소형기관의 송금을 자기 플랫폼으로 모아 대신 접속하는 대형 핀테크 사업자. 여러 사람의 소포를 모아 한 트럭으로 실어 나르는 집하장과 같다.

→ 전용계좌는 **수십 개 수준**으로 거액(134개)보다 오히려 적다. 하루 수백만 건이 이 좁은 줄에 몰리므로 핫 계좌 집중(2.3)은 더 심해지며, 저널 순차처리가 이를 흡수한다는 논거는 그대로 유효하다.

접속 방식 — "대표주소 하나로 여러 센터" 사상, 단 경로별로 실현 수단이 다르다

참가기관이 여러 센터를 각각의 주소로 관리하게 하면 운영 부담과 설정 오류 위험이 커진다(참가기관이 평상시 접속하는 곳은 근거리 3센터이며, 대전 DR은 광역재해 때만 쓰이는 최후보로라 상시 접속 대상이 아니다). 따라서 **참가기관은 논리적으로 "하나"만 바라보고, 어느 센터로 연결할지는 한국은행 쪽이 정한다**는 사상(과제 ⑦ 계승, FedNow의 "여러 지점이나 접속은 하나로 보임"과 동일)을 택한다.

중요한 구분 — 이 "하나로 보이게" 하는 일은 두 가지 서로 다른 기술로 실현되며, 경로에 따라 주력이 다르다. 흔히 "MQ(메시지 큐, 전문을 큐에 쌓아 순서대로 전달하는 미들웨어)를 쓰면 GSLB가 필요 없다"고 하는데, 이는 절반만 맞다. GSLB와 MQ는 **대체 관계가 아니라 서로 다른 계층**이기 때문이다.

먼저 쉬운 비유: GSLB는 "여러 센터 중 어디로 접속할지 자동 안내하는 교통정리 요원"(연결을 *맺기 전* 단계)이고, **MQ 페일오버**는 "일단 연결된 뒤 오가는 편지를 한 통도 잃지 않게 지키는 장치"(연결을 *맺은 후* 단계)다. 둘은 하는 일이 겹치지 않는다.

구분	GSLB(대표주소·로드밸런서)	MQ 클러스터 페일오버(메시지 큐 자체 기능)
푸는 문제	"어느 센터로 붙을지"를 정해줌(연결 지점 탐색)	붙은 뒤 " 메시지를 잃지 않고 순서대로 " 주고받기
동작 층위	DNS·네트워크(연결 성립 *이전*)	세션·애플리케이션(연결 성립 *이후*)
전환 방식	DNS 응답을 바꿔 새 센터로 유도	브로커가 연결 목록으로 살아있는 노드에 자동 재연결

"MQ가 GSLB를 대체한다"의 진실: MQ 미들웨어에는 **참가기관 프로그램이 "접속 가능한 센터 명단"을 미리 갖고 있다가, 붙어 있던 센터가 죽으면 명단의 다음 센터로 스스로 옮겨 붙는 기능**(연결 목록 기반 자동 재연결)이 내장돼 있다. 그래서 **결제 전문 경로에서는 별도 GSLB 장비 없이도 무중단 접속이 성립**한다(FedNow·TIPS가 실제로 이 방식). 즉 GSLB 기능이 사라진 게 아니라 **MQ 안으로 흡수된 것**이다. 그리고 결제 전문의 **순서 보장·무손실 전달**은 MQ의 본연 기능이므로, 결제 경로엔 이쪽이 더 정합적이다.

→ 따라서 본 보고서는 **경로별 분담**을 택한다(2.6의 "같은 도구도 어디에 쓰느냐" 원칙과 정합):

경로	주력 수단	이유
결제 전문 (잔액을 바꾸는 지시)	MQ 클러스터 페일오버	순서·무손실·자동 재연결이 MQ 본연 기능 — 결제 경로의 정석(FedNow형)
접속·인증·조회·관리 API	GSLB(대표주소)	상태 없는 요청·웹형 접속엔 DNS 기반 유도가 단순·익숙

공통 원칙: 어느 수단이든 그 계층 자체가 새 단일점이 되지 않도록 근거리 3센터에 분산 배치(이중화)하고, 어디로 붙어도 같은 판단을 하도록 센터 상태를 공유한다. 채택 조건도 동일하다 — 거래 처리시간에 유의미한 지연을 더하지 않을 것(BMT로 확인, 6.4).

참가기관 관점 대안 비교(위 분담을 전제로). 결제 경로에서 참가기관이 실제로 마주하는 선택은 "대표 접속(한은가 전환 처리)" 대 "복수 주소 직접 관리"다.

항목	본안 A — 대표 접속(MQ 클러스터 페일오버 / GSLB)	대안 B — 복수 주소 명시
참가기관 관리	논리 접속 1개(연결 목록은 규약이 배포)	센터별 주소 + 우선순위 재시도 로직 직접 구현
부하·전환	중앙에서 동적 조정·자동 전환(설정 변경 불요)	참가기관별 고정(쓸림 위험)·재시도 구현에 의존
약점	접속 계층 자체의 장애·지연(→ 이중화로 방어)	기관별 구현 편차·설정 오류

확인(6.4 BMT #5) 전까지 본안 A가 후보이며, 오버헤드가 크면 대안 B로 전환한다.

장애 시 참가기관에 보이는 것 — 단일 장애는 거의 안 보이게, 극단 상황은 예측 가능하게

상황	시스템 동작	참가기관 체감
평상시	세 센터로 분산 접속	정상
근거리 1개 상실	나머지 2개가 정족수 유지, 접속 자동 재라우팅	순단 후 자동 재접속 (수 초), 미응답 거래는 먹통 재전송
근거리 2개 동시 상실	잔존 1센터는 정족수 미달로 안전 정지 (이중지급 방지를 위한 의도된 정지) → 사람 판단으로 대전 DR 가동 또는 잔존 센터 단독 재구성 (마지막 과반 확정 순번까지 보유했는지 검증 후 — 미보유분은 저널 복구·대사로 회수)	일시 중단 → 재개 (분 단위)
수도권 광역재해(3개 상실)	대전 DR 가동(비동기, RPO>0)	분 단위 중단 후 재개

- 왜 이 극단 상황만 사람이 결정하는가.** 단일 센터 상실은 판정이 명확하고 무슨일이라 자동이 안전하다. 반면 근거리 2개 동시 상실·광역재해는 극히 드문 데다 **데이터 손실(RPO>0)이나 정족수 재구성을 감수할지의 결정**을 포함한다. **손실을 수반할 수 있는 결정은 자동화하지 않고 사람이 내린다** — 과제 ②의 "결정은 사람" 원칙이 이 극단 시나리오에는 그대로 유지된다(판단 시한·당직 체계는 운영 설계 (3.3·⑩)에서 정한다).
- 재접속 "수 초"와 RTO≈0은 모순이 아니다.** RTO≈0은 "시스템이 복구 과정 없이 처리를 이어간다"는 뜻이고, 개별 참가기관의 연결이 살아있는 센터로 옮겨 붙는 데는 수 초가 걸릴 수 있다. 그 공백에 떠

있던 거래는 **고유번호 역등 재전송**(2.4)이 "정확히 한 번"으로 흡수한다 — 과제 ⑦의 "불확실하면 같은 번호로 다시" 규칙 그대로다.

- **대전은 정족수에 참여하지 않는다.** 근거리 3센터가 자체로 흡수(3표)를 이루므로 별도의 심판이 필요 없다. 따라서 **대전 구간 회선 장애는 평상시 결제 처리에 아무 영향을 주지 않으며**, 대전과는 비동기 복제 회선만 유지하면 된다(역할은 2.1 그대로 — 광역재해 최후보루 전용).

참가기관 행동 규약 — 과제 ⑦ 적합성 인증의 계승

접속이 참가기관에게 "투명"하려면 참가기관 클라이언트도 규약을 지켜야 한다. 과제 ⑦에서 확립한 표준을 소액 RTGS 접속 규격에 그대로 계승한다 — **대표주소만 사용(특정 센터 주소 하드코딩 금지) · 자동 재접속(동시 폭주 방지용 분산 지연) · 모든 지시에 고유번호 · 불확실 시 같은 번호로 역등 재전송 · 재접속 후 상태 조회**, 그리고 운영 투입 전 **적합성 인증** 통과. 애그리게이터는 트래픽 변동성이 가장 크므로 **스파이크 상황의 재접속·재전송 폭주 시험**을 인증 항목에 추가한다.

대외 접점 보안(요지). 폐쇄망·전용회선이 기본이지만, 24/365 대외 접점(접속 게이트웨이·입구)과 참가기관 확대는 공격 표면을 넓힌다. 접속 규격에 **참가기관 상호인증(mTLS)·전문 전자서명(ISO 20022)·회선 암호화**를 포함하고, 위협 모델에 **폭주 공격(DDoS)·참가기관 계정 탈취·저널 오염 공격**을 넣어 국제 사이버 복원력 기준(CPMI-IOSCO, 과제 ② 계승)과 정합시킨다. 상세 보안 통제와 센터 간 회선 보호는 보안 설계·과제 ⑨(네트워크)에서 다룬다.

참가기관 측 24/365 대응. 한국은행 측이 무중단이어도, 각 은행 코어뱅킹에는 야간 점검·일 마감 시간대가 있다 — 은행 20곳이 이를 못 맞추면 고객 체감 서비스는 어차피 끊긴다. 해외 사례(FedNow)처럼 **참가기관별 점검창을 제도화**하고, 점검창 중 수신되는 거래의 처리 규칙(지연 게시 등)을 접속 규격에 포함한다. 참가기관의 준비도·비용·이행 일정은 참가 제도 설계(6.1-12)와 함께 조사한다.

2.6 신기술 적용가능성 평가 — 인메모리 DB·RDB·API·클라우드

왜 이 평가가 필요한가

해외 중앙은행 RTGS 사례를 검토하면 **인메모리 DB(NoSQL)·RDB·API·클라우드** 같은 신기술이 빠짐없이 등장한다. 그래서 "이 최신 기술들만 쓰면 빠르고 안정적인 시스템이 저절로 만들어진다"는 기대가 생기기 쉽다. 그러나 **정보계(조회·분석)나 일반 핀테크에서 우수한 기술이, 계정계(돈을 직접 기록하는 영역)인 RTGS에서는 오히려 독이 되는 경우가 많다.** 따라서 각 기술을 무비판적으로 받아들이지 않고, 소액 RTGS의 두 절대 요건 — **이중지급 방지(정확성)와 무중단(RTO≈0)** — 에 비추어 적용 가능 여부를 가린다.

먼저 잡아야 할 대전제 — 속도와 안정성은 양립하기 어렵다. 처리 속도를 높이는 기술(인메모리)은 대체로 안정성을 낮추고, 안정성·범용성을 높이는 기술(분산처리·API·클라우드)은 대체로 속도를 늦춘다. **둘 다 최고로 잡는 시스템은 없다.** 소액 RTGS는 "사용자 체감 속도(이체 속도)"도 중요하지만, 중앙은행 인프라인 이상 **정확성·무중단이 항상 우선**이다. 이 우선순위가 아래 모든 판정의 기준이다.

종합 평가표

각 기술을 **결제 확정 경로**(잔액을 실제로 깎고 더하는 원장의 심장부)와 **부가 경로**(전문 수신·접속·조회·분석 등 주변부)로 나누어 평가한다. 같은 기술도 어디에 쓰느냐에 따라 적합/부적합이 갈리기 때문이다.

기술	결제 확정 경로(원장)	부가 경로 (입구·접속· 조회)	종합 판정	핵심 근거
인메모리 DB / NoSQL	× 부적합	○ 적합	조건부	원장은 정확·내구성이 생명 → RDB. 전문 입수·조회 사본엔 인메모리·문서형이 적합
RDB(관계형 DB)	○ 적합	△ 무관	적합 (원장의 정답)	잔액 정합성·강한 일관성·내구성의 표준. 토스뱅크 등 국내 인터넷전문은행 계정계도 RDB
API	× 부적합	○ 적합	조건부	잔액 확정엔 전문(ISO 20022) 교환이 정석. 접속·조회·관리에는 API가 유효
클라우드(공용)	× 제약	△ 제약	현 단계 부적합	한국은행 폐쇄망·보안승인·원격관리 제약과 충돌. 사상(수평확장)만 사설 인프라에 차용

기술별 상세

(1) 인메모리 DB / NoSQL — "속도 만능"은 오해, 원장엔 부적합

인메모리 DB는 데이터를 디스크가 아닌 메모리에 두어 빠르게 처리하는 기술이고, NoSQL은 정형화되지 않은 데이터(거래 전문 같은 텍스트)를 유연하게 다루는 데이터 모델이다. (둘은 흔히 한 묶음으로 언급되나 **서로 다른 축**이다 — 인메모리는 "어디에 저장하나", NoSQL은 "어떤 모양으로 저장하나"의 문제다.)

- **원장(잔액 확정)에는 부적합하다.** 잔액은 단 1원도 틀리면 안 되고(정확성), 전원이 나가도 사라지면 안 된다(내구성). 인메모리·NoSQL은 흔히 **최종적 일관성**(지금은 달라도 잠시 후 같아짐)을 기본으로 하는데, 이는 결제에 치명적이다(2.3절의 이중지급 경고와 동일 논리). 계정계 데이터는 **RDB**가 정석이다.
- **속도 향상 효과도 과장되기 쉽다.** 한 건의 거래를 처리하는 전체 시간 중 "전문을 받아 메모리에 넣는" 단계가 차지하는 비중은 작다. 따라서 인메모리를 도입해도 **체감 속도가 기대만큼 빨라지지 않는다.**
- **그럼에도 쓸 자리는 있다.** 폭주하는 거래 전문을 **빠르게 받아 줄 세우는 입구**(2.4절 메시지 큐)와, 확정된 결과의 **읽기 전용 조회·분석 사본**(2.3절 문서형 DB)에는 적합하다. 해외 중앙은행의 "인메모리 그리드"도 속도보다 **무상태(stateless) 복원력** — 노드가 죽어도 빈자리를 다른 노드가 즉시 메우는 구조 — 를 위해 쓰는 것으로, "빨라서"가 아니다.

→ 판정: 조건부 — 입구·조회 사본엔 쓰되, 원장 확정에는 쓰지 않는다. (이미 2.3·2.4절에 반영된 역할 분리 원칙을 재확인.)

(2) RDB — 계정계 원장의 정답

관계형 DB(RDB; 오라클·PostgreSQL 등)는 잔액의 강한 일관성·내구성을 보장하는 데이터 처리의 표준이다. **소액 RTGS의 권위 잔액 원장은 RDB로 구현하는 것이 정석**이며, 국내 인터넷전문은행도 계정계 핵심 업무는 RDB를 쓴다. 우리 보고서가 2.3절에서 "강한 일관성 엔진"이라 부른 것의 실체가 바로 이 RDB 기반 원장이다.

오픈소스 RDB에 대한 균형 잡힌 시각(2026년 기준). 한때 "오픈소스 DB(PostgreSQL 등)는 이중화(고가용성) 구성이 취약하다"는 평가가 있었다. 그러나 **2026년 현재 PostgreSQL은 동기 스트리밍 복제와 자동 페일오버 도구(Patroni 등)를 통해 고가용성 구성이 가능하며,** 국내 금융권(인터넷전문은행 계정계 포함)에서 실운영되고 있다. 다만 24/365 중앙은행 인프라라는 최고 수준의 무중단·무손실 요건에서 **상용 DB 대비 운영 성숙도·장애 복구 검증 실적은 별도로 확인**해야 한다. 즉 "오픈소스는 무조건 불가"도, "오픈소스로 충분"도 아닌 — **PoC로 검증할 사안**이다.

→ 판정: 적합 — 원장은 RDB. 오픈소스 채택 여부는 운영 성숙도 검증(PoC) 후 결정.

(3) API — 접속·조회엔 유효, 잔액 확정엔 부적합

API는 불특정 다수에게 표준화된 방식으로 기능을 열어주는 기술로, **범용성·연계 편의성**이 강점이다. 그러나 RTGS 같은 계정계 업무는 거래 상대방의 **신원 확인이 필수**라 거래 전에 정해진 양식의 **전문(ISO 20022 표준 메시지)을 교환**하는 것이 정석이다. 따라서 **잔액을 실제로 확정하는 결제 경로에 API를 쓰는 것은 적합하지 않다**(범용성을 얻는 대신 속도·엄밀성을 잃는다).

단, "API는 RTGS에 모순"이라는 전면 부정은 과도하다. 부정되는 것은 어디까지나 **결제 확정 경로**다. 참가기관의 **접속·인증, 잔액·거래내역 조회, 시스템 운영·관리**에는 API가 오히려 효율적이며, 미연준 FedNow도 ISO 20022 전문(결제)과 운영 API(접속·관리)를 **병행**한다. 핵심은 "API냐 전문이냐"의 양자택일이 아니라 **경로별로 맞는 도구를 쓰는 것이다**.

→ 판정: 조건부 — 결제 확정은 전문(ISO 20022), 접속·조회·관리는 API.

(4) 클라우드 — 사상은 차용, 공용 클라우드는 현 단계 부적합

클라우드(범용 x86 서버 기반)는 자원을 유연하게 늘렸다 줄였다 하는 **확장성·범용성**이 강점이다. 그러나 소액 RTGS에 **공용(public) 클라우드를 직접 적용하기에는 제약이 크다**.

- **보안·규제 제약:** 한국은행 핵심 결제 인프라는 **폐쇄망** 운영이 원칙이고, 망분리·보안승인 대상이다. 또한 **현재 국가정보원은 중요 시스템의 원격 관리를 허용하지 않아,** 이탈리아 중앙은행처럼 "무인 운영 + 원격 관리"를 그대로 따라갈 수 없다(이는 운영 이슈⑦·법적 제약과도 연결된다).
- **속도 측면:** 범용 인프라 위에 분산 구조를 얹으면 통신·동기화 지연이 더해져 결제 속도가 늦어질 수 있다.

→ 판정: 현 단계 공용 클라우드 직접 적용은 부적합. 다만 "필요한 만큼 노드를 늘리는 수평 확장(scale-out)" 사상은 유효하므로, 이를 **한국은행 사설 인프라(전용 데이터센터) 위에서 구현**한다(2.2절 확장성 원칙과 동일). 즉 클라우드의 *기술*이 아니라 *설계 사상*만 차용한다.

평가가 주는 시사점 — "신기술 톤(수위) 조절"과 거버넌스

이상의 평가에서 일관되게 확인되는 것은, **신기술은 "쓰느냐 마느냐"가 아니라 "어디에 어떤 역할로 쓰느냐"의 문제**라는 점이다. 같은 인메모리도 입구에는 약이고 원장에는 독이며, 같은 API도 조회에는 유효하고 확정에는 부적합하다. 따라서 마스터플랜·대외 보고에서 신기술을 다룰 때는 "**이 기술들을 적용하면 빠르고 안정적인 시스템이 가능하다**"는 식의 단정을 피하고, "**해외 사례의 신기술에 대해 우리 환경에서의 적용 가능성을 경로별로 검토한다**"는 수준으로 톤을 조절하는 것이 바람직하다.

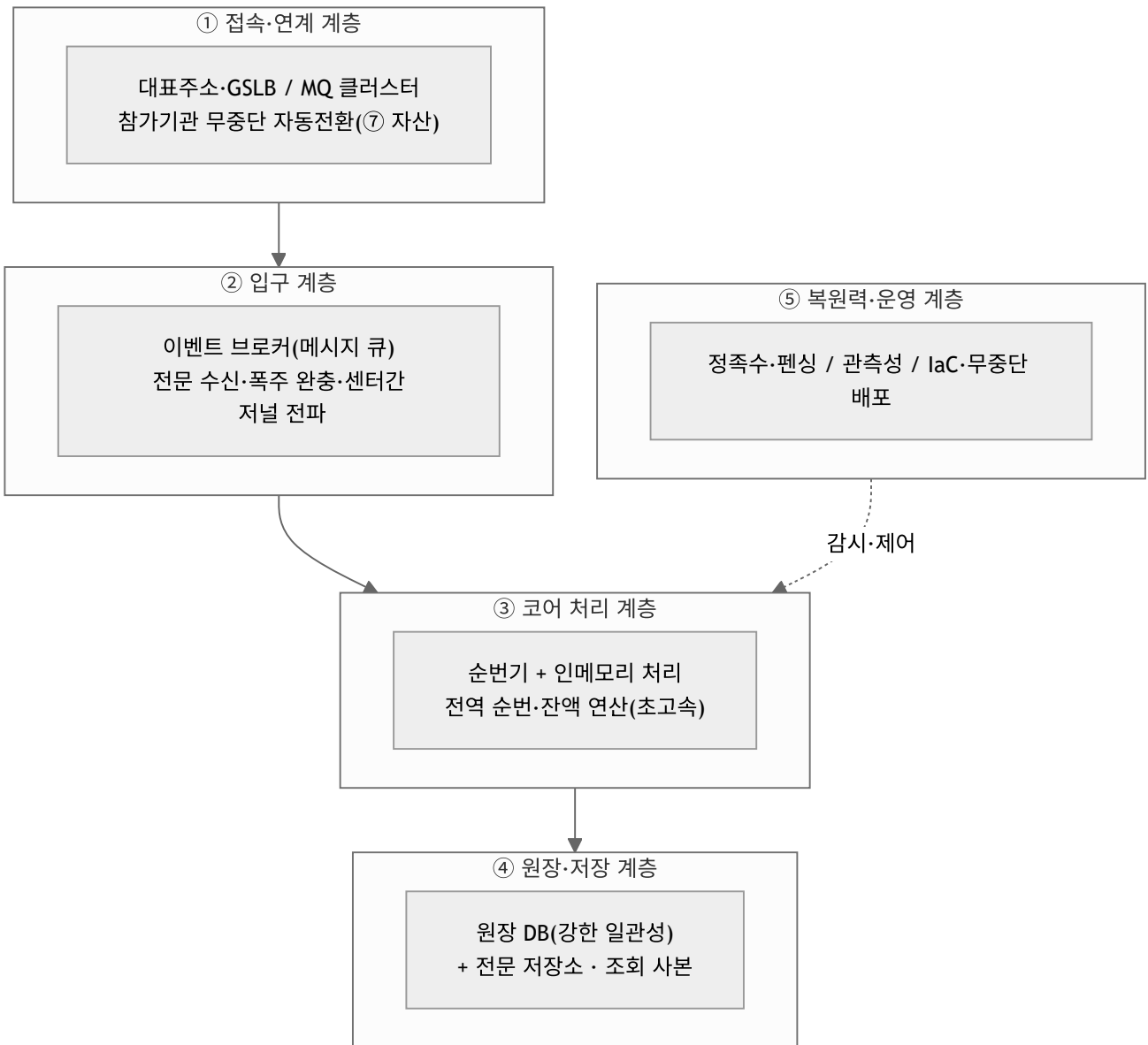
또한 소프트웨어 기반 Active-Active는 분산·동기화로 인한 **거래 처리시간 지연이 필연적**이므로, 이를 추상적 약속이 아니라 **PoC(개념검증)로 실제 측정**하고, 그 결과를 바탕으로 **IT전략국과 금융결제국 사이에 "허용 가능한 처리시간"에 대한 공감대를 먼저 형성**해야 한다(5장 확인필요·거버넌스 항목에 반영). 비즈니스 요구(어떤 모델·어떤 처리시간을 목표로 하나)가 먼저 확정되어야 그에 맞는 기술요소가 정해진다 — **기술이 비즈니스를 끌고 가는 것이 아니라 그 반대다.**

2.7 기술 스택 구성 — 무엇으로 이 구조를 보장하는가 (★스택)

앞 절들이 "어떤 구조로 무중단·무이중지급을 이룰 것인가"를 논했다면, 이 절은 그 구조를 **실제로 어떤 계층의 어떤 종류의 솔루션으로 구현하는가**를 정리한다. 핵심 원칙은 하나다 — **각 계층의 요구가 다르므로, 한 가지 만능 도구가 아니라 계층마다 그 역할에 맞는 도구를 배치**한다(2.3·2.6의 "어디에 쓰느냐" 원칙의 구체화).

먼저 짚을 것 — 아래 제품명은 "유형의 예시"이지 특정 제품 지정이 아니다. 결제 인프라의 솔루션 선택은 성능·안정성뿐 아니라 **국산화·벤더 중속·보안승인·기술 내재화** 등 정책 변수가 함께 걸린다. 따라서 본 절은 **계층별로 "어떤 성질의 도구가 필요한가"**를 규정하고, 구체 제품은 PoC-BMT로 검증해 확정한다.

계층별 기술 스택



계층	역할	필요한 도구의 성질	유형 예시
① 접속·연계	참가기관 접속·장애 시 무중단 자동전환	대표주소 기반 자동 라우팅, 소스 수정 없이 설정 배포로 전환	GSLB·사설 DNS / MQ 클러스터 페일오버(과제 ⑦ 자산 재사용)
② 입구 (이벤트 브로커)	전문 수신·폭주 완충·센터 간 저널 전파	고처리량 메시지 스트림, 센터 간 순서 보존 복제	메시지 큐/이벤트 브로커류
③ 코어 처리	전역 순번 부여 + 잔액 연산	초저지연 순차처리(메모리), 결정론적 재생	인메모리 처리 엔진 + 시퀀서(자체 개발 영역)
④ 원장 DB	잔액의 최종 확정·보관	강한 일관성·내구성(단 1원도 틀리면 안 됨)	관계형 DB(RDB) — 국산/상용/오픈소스는 성숙도 검증 후(2.6)

계층	역할	필요한 도구의 성질	유형 예시
④-보조	원전문 보관·조회·분석 사본	대용량·유연 스키마(정합성 요구 낮음)	문서형/NoSQL DB
⑤ 복원력·운영	정족수 판정·펜싱, 감시, 무중단 배포	자동 장애판정, 관측성, 코드형 인프라	정족수 합의(3센터 홀수 구성)·펜싱 / 관측성 스택 / IaC·배포 도구

계층별 설계 원칙 (왜 이 성질이라야 하나)

① **접속·연계** — **"참가기관은 아무것도 바꾸지 않는다"**. 한 센터가 죽어도 참가기관이 접속 설정을 바꾸지 않고 자동으로 살아있는 센터에 붙어야 한다(참가 구성·접속 규약은 2.5). 2.5에서 정한 **경로별 분담**이 이 계층의 구체다 — **결제 전문은 MQ 클러스터 파일오버, 접속·조회·관리 API는 대표주소·GSLB**(과제 ⑦ 자산)가 각각 주력이다. 어느 쪽이든 **소스 수정 없이 설정 배포만으로 전환**되는 것이 핵심 — 참가기관 부담을 0으로 만든다.

② **입구(이벤트 브로커)** — **"완충 + 순서 보존 전파"**. 전 국민 트래픽이 순간 폭주(스파이크)해도 코어가 무너지지 않도록 앞단에서 완충한다. 동시에 **순번이 매겨진 저널을 세 센터에 순서 그대로 전파**하는 통로 역할을 한다. 이 계층은 최종적 일관성이어도 무방하다 — **순서의 권위는 순번기가 쥐고**, 브로커는 전달만 하기 때문이다(그래서 브로커에 원장 확정을 맡기면 안 된다, 2.3 경고).

③ **코어 처리** — **"한 줄로, 그러나 메모리에서 초고속으로"**. 전역 순번 부여와 잔액 연산은 순차처리(한 줄)라 처리량의 상한을 만든다. 이를 메모리 상에서 처리해 한 건당 시간을 극한으로 줄이고, 그 앞뒤(형식 검증·전문 생성·송신)는 병렬화한다. **이 코어는 시스템의 심장이자 가장 특수한 영역이므로 완전한 기술 내재화(자체 개발) 대상**이다(2.6 시사점의 "핵심 로직 내재화").

④ **원장 DB** — **"여기만은 타협 없는 강한 일관성"**. 잔액의 최종 확정·보관은 **관계형 DB(RDB)**로 한다. 인메모리에서 연산하더라도, 그 결과의 **권위 있는 최종본은 반드시 강한 일관성·내구성을 보장하는 원장에 확정**한다(전원이 나가도 사라지면 안 됨). 원전문(ISO 20022 XML)과 조회·분석 사본은 별도의 문서형 DB로 분리해 코어의 부담을 덜는다.

⑤ **복원력·운영** — **"구조를 지키는 자동 장치"**. 정족수·펜싱(2.1·2.3)이 장애를 자동 판정·격리하고, 관측성 체계가 상태를 상시 감시하며, 코드형 인프라(IaC)·무중단 배포가 사람 손을 최소화한다(3.3에서 상술). 특정 벤더 종속을 줄이기 위해 이 계층은 **공개 표준·오픈소스 기반**을 우선 검토한다.

경량 명령문 — 세 센터 복제를 빠르게 하는 열쇠

세 센터가 저널을 주고받는 양이 많을수록 지연이 커진다.

쉬운 비유: 무거운 원본 편지(수십 KB의 전문)는 창고(별도 저장소)에 두고, 세 센터끼리는 **요점만 적은 쪽지(수백 바이트)만 주고받는다**. 쪽지가 가벼우니 세 센터를 오가는 속도가 빨라진다.

따라서 참가기관이 보낸 **원전문(최대 수십 KB의 XML)**은 **입구에서 별도 저장소에 보관**하고, 세 센터 사이에는 **원장 연산에 꼭 필요한 최소 정보만 추출한 경량 명령문**(금융기관 식별자·계좌·금액·원전문 해시 등 수백 바이트)을 복제한다. 각 센터 코어는 무거운 텍스트 해석을 생략하고 이 경량 구조체만

순서대로 처리하므로 복제·처리 속도가 극대화된다. 원전문 해시(위변조 방지 지문)를 함께 실어 무결성·부인방지도 확보한다.

요약: 기술 스택의 요체는 "만능 도구 하나"가 아니라 "계층마다 맞는 도구"다. 폭주 완충은 이벤트 브로커, 순서·속도는 인메모리 순번기, 정확·내구는 RDB 원장, 조회는 문서형 DB, 무중단은 정족수·laC가 각자 맡는다. 그리고 **가장 특수한 코어(순번기·원장 엔진)는 자체 개발로 내재화**하고, 주변부는 검증된 오픈소스·상용을 혼합해 효율을 높인다.

3. 핵심 운영 이슈와 대응방안

기술만큼 중요한 것이 운영이다. 24/365 무중단 시스템은 "만드는 것"보다 "멈추지 않고 운영하는 것"이 더 어렵다.

3.1 이슈⑤ 마감 없는 무결성·대사

이슈

기존 시스템은 매일 **마감 시점**에 하루치 장부를 맞춰보고(대사), 정리하고, 백업했다. 그런데 **24/365 즉시지급에는 마감이 없다**. 영원히 돌아간다. **점검할 한가한 시간이 사라진** 것이다.

비유: 달리는 기차 안에서 멈추지 않고 바퀴를 점검하고 갈아 끼워야 하는 상황이다.

특히 위험한 것은 **논리적 오염**(버그·운영자 실수로 잔액이 잘못 기록되는 것)이다. 저널을 세 센터가 함께 재생하는 구조에서는 오염된 거래도 세 센터에 똑같이 반영되므로, **오염을 늦게 발견할수록 피해가 커진다** (과제 ②에서 확인: "탐지 시간 = 피해 규모").

대응방안 — 상시 대사 + 오염 탐지 3겹 (과제 ② 계승)

마감 대사를 **상시(실시간) 대사**로 전환한다. 과제 ②에서 설계한 **오염 탐지 3겹**을 24/365에 맞게 개조해 적용한다.

겹	방법	24/365 적용
1겹	상시 대사	마감 일괄 대신 흐르는 중에 연속 검증
2겹	무결성 검증	잔액 합계·전문 정합성 실시간 점검
3겹	이상 탐지	비정상 패턴(급증·역전) 자동 경보

복구는 단순 롤백이 아니라 **에어갭 백업(복제와 분리된 별도 백업)**에서 **오염 직전 시점으로 선별 복구**한다. 국제기준(CPMI-IOSCO)도 "신뢰할 수 있는 상태로 2시간 내 회복"을 요구한다. 다만 24/365라 "되감을 마감"이 없으므로, **시점 복구 지점(체크포인트)을 짧은 주기로 연속 생성**하는 설계가 추가로 필요하다.

왜 "디스크 통째 복제"가 아니라 "거래 명단(저널) 복제"인가 — 스토리지 복제의 함정. 세 센터에 데이터를 복제하는 방법은 크게 두 층위가 있다. 디스크(스토리지)를 통째로 복제하는 방식과, 거래 명단(저널)을 애플리케이션이 복제하는 방식이다(2.1-2.3에서 후자를 택했다). 스토리지 통째 복제가 단순해 보이지만 결제에는 부적합하며, 그 이유가 우리 노선 선택의 근거이기도 하다.

스토리지 복제의 함정	무슨 일이 벌어지나	쉬운 설명
미확정 거래 부활	DB가 "아직 확정 안 함"이라 표시한 거래를 스토리지는 그 표시를 못 읽고 복제 → 장애 후 유령처럼 살아남음	지우다 만 낙서가 사본엔 지워지지 않고 남는 격
오염의 즉시 전이	원본이 손상되면 스토리지는 손상 상태 그대로 사본에 복제	원본 오타를 검토 없이 그대로 복사
순서 뒤엎김	잔액과 거래기록이 다른 디스크에 있을 때 복제 시점이 어긋나면 선후 관계가 깨짐	입금 기록만 복사되고 출금 기록은 아직인 순간에 사고

저널(거래 명단)은 "무슨 거래를 어떤 순서로"라는 **논리적 의미**를 담고 있어, 위 함정을 피하고 필요 시 그 명단을 다시 재생해 정확히 복구할 수 있다. 그래서 본 과제는 스토리지가 아니라 **애플리케이션 층위의 저널 복제**를 택한다. (이 논거는 과제 ②의 복원력 설계와도 직결된다.)

3.2 이슈⑥ 24/365 유동성 관리

이슈

건별 즉시 완결(RTGS)을 하려면, 그 순간 차감할 **잔액이 참가기관 전용계좌에 미리 들어 있어야** 한다. 그런데 24/365라 **야간·주말에도 유동성이 필요하다**. 기존에는 영업시간에만 신경 쓰면 됐던 결제유동성을, 이제 **밤낮·휴일 없이** 관리해야 한다. 이는 참가기관에 새로운 부담을 준다(한국은행도 RTGS 전환의 핵심 과제로 인식하고 있다).

대응방안 — 사전예치(참가기관 자율) + 일중당좌대출 보전

- **사전예치(prefunding)**: 참가기관이 전용계좌에 결제용 자금을 미리 예치하고, 거래마다 그 잔액을 실시간 증감한다. (TIPS-FedNow의 실제 운영 방식.) **예치 규모는 한국은행이 강제하는 것이 아니라 참가기관이 자기 거래량·리스크를 보고 자율적으로 결정한다**.
- **일중당좌대출로 부족분 보전**: 예치금이 일시적으로 부족해도 거래가 막히지 않도록, **일중당좌대출 (한국은행이 일중에 일시 자금을 공급하는 제도)을 이용할 수 있다**. 즉 참가기관은 "필요한 만큼만 예치하고, 순간 부족분은 일중당좌대출로 메우는" 방식으로 유동성 부담을 조절한다.
- **★ 애그리게이터(비은행 직접 참가자)의 유동성 공백**: 일중당좌대출은 현행 제도상 **은행(한은 당좌예금 거래 기관) 대상**이다. 트래픽 비중·변동성이 가장 크다고 본 보고서 스스로 규정한 애그리게이터(2.5)는 이 안전판 없이 **사전예치에 전액 의존**하게 되거나, 비은행의 중앙은행 계좌·유동성 접근을 새로 설계해야 한다(한국은행법·관련 규정 정비 사안). 참가 구성(6.1-12)과 묶어 **정책 트랙의 핵심 쟁점**으로 다룬다.

- **남은 검토점:** 일종당좌대출이 영업시간 중심으로 운영되어 온 만큼, **24/365 가동(야간·주말)에서의 운영 방식**은 추가 검토가 필요하다. 이는 시스템 설계만의 문제가 아니라 **참가기관 협의·제도 운영**이 수반되므로, 기술 구축과 **병행하는 정책 트랙**으로 다룬다.

3.3 이슈⑦ 무중단 운영·배포

이슈

시스템을 고치거나 업그레이드하려면 보통 잠깐 멈춘다. 그런데 **멈출 수가 없다**. 또한 야간·주말 사고에 대응할 인력이 항상 대기하기 어렵다.

대응방안 — 무중단 배포 + 야간 자동 대응 (과제 ⑩ 계승)

- **무중단 배포(rolling deployment):** 근거리 3센터 동시 가동을 활용해, 한 번에 한 센터(또는 일부 노드)만 순차적으로 교체하고 그동안 나머지 두 센터가 처리를 이어받는다. 변경의 위험 수준에 따라 배포 방식을 차등한다.

변경 규모	배포 방식	쉬운 설명
소규모 패치	롤링 + 기능 스위치 (Feature Flag)	배포와 "켜는 시점"을 분리 — 코드는 미리 깔되 스위치로 나중에 활성화
기능 변경	카나리(Canary)	소수 트래픽(1~5%)에 먼저 적용해 이상 없으면 전체 확대
DB 스키마 변경	확장-수축(Expand-Contract)	신·구 구조를 잠시 공존시켜 무중단 유지 후 옛 구조 제거
대규모 고위험	센터 단위 전환	한 센터 트래픽을 전량 뺀 뒤 작업, 끝나면 복귀

이렇게 하면 **대부분의 변경을 서비스 중단 없이** 수행할 수 있고, 불가피한 대규모 변경만 **자정 전후 계획 점검창(10~20분, 이슈④)**을 병행한다.

배포 중 정족수 유의. 센터 단위 전환으로 한 센터를 통째로 빼면 그동안 시스템은 2센터 상태가 된다 — 이 시간창에 추가 장애가 1건만 나도 정족수 미달로 전면 정지다. 따라서 ① 기본은 **센터 전체가 아닌 노드 단위 롤링**(센터는 정족수에 계속 참여)으로 하고, ② 불가피한 센터 단위 이탈은 최저 트래픽 시간대에 최단으로 제한하며, ③ 이탈 센터의 신속 복귀(저녁 따라잡기) 절차를 사전에 리허설한다.

- **야간·주말 자동 대응:** 과제 ⑩(IT 인프라 자동화)에서 설계한 "**실행은 자동, 결정은 사람**" 운영 자동화를 계승하되, 이슈①에서 본 대로 **장애 전환은 자동 판단(정족수)**으로 한 단계 더 끌어올린다. 사람은 사후 확인·예외 처리에 집중한다.
- **관측성·코드형 인프라(참고):** 무중단 운영의 토대로, 시스템 상태를 상시 들여다보는 관측성 체계와 인프라를 코드로 관리하는 방식(IaC)을 함께 둔다. 벤더 종속을 줄이기 위해 공개 표준·오픈소스 기반을 우선 검토한다(구체 스택은 2.7·과제 ⑩과 연동).

4. 국제 벤치마크 종합 — 무엇을 बे끼고, 무엇을 못 베끼나

해외의 RTGS 방식 즉시지급 시스템을 객관적으로 비교한다. 핵심은 "이식 가능한 것과 불가능한 것을 가리는 것"이다.

항목	TIPS (유럽중앙은행)	FedNow (미연준)
가동	2018년(2023년 3센터 A-A-A로 개편)	2023년
목표 처리량	초당 2,000건(확장 가능)	미공개(보안)
응답 속도	규정상 99%를 5초 이내(실측은 100ms 이하)	"밀리초 단위"
가용성 목표	99.9%	24×7×365(수치 비공개)
복구목표 (RTO)	0(3센터 A-A-A 개편 후 실증)	비공개
센터 구성	근거리 3센터 A-A-A(동기복제 거리 내)	광역 분산형 다중센터
잔액 기록	인메모리 잔액 + 강한 일관성 저장 (3센터 동시재생)	분산 인메모리 그리드(구현 사례 기준)
외부 접속	중앙 집중	"여러 지점이나 접속은 하나로 보임"(우리 ⑦ GSLB와 동일 사상)

무엇을 차용할 수 있나:

벤치마크 요소	차용 가능성	설명
TIPS의 근거리 3센터 A-A-A(RTO=0)	◎ 본안 채택	우리 근거리 3센터(남대문/IDC) 구조의 직접 모범 — 이슈①
TIPS의 저널 순차처리·인메모리 코어	○ 사상 차용	이중지급·순서변경 원천 차단 — 우리 이슈③·2.3 정합
TIPS의 정량 목표(2,000 TPS·확장·5초·99.9%-RTO 0)	○	처리량도 우리 현행 피크와 같은 2,000 기준선 + 확장 — 방향 일치
TIPS 소프트웨어 자체	×	ECB 전용. (RIX-INST처럼 TIPS에 가입하는 길은 주권·통화 문제로 비현실적)
FedNow의 단일접속·다지점 사상	○	이미 우리 과제 ⑦(GSLB) 자산 — 재사용
FedNow 내부 TPS·아키텍처	×	미공개(단, 일평균 처리량은 아직 신생·소규모로 공개)
FedNow 클라우드 네이티브	△	한국은행 폐쇄망·보안승인 제약과 충돌

벤치마크의 결론 — "넘어서기"가 아니라 "정확히 쫓기". 검토 결과 유럽 TIPS는 이미 **근거리 3센터 A-A-A-RTO=0.2,000 TPS(확장 가능)**를 실증한, 우리가 지향하는 바를 그대로 구현한 선진 사례다. 따라서 본 과제의 목표는 국제 모범을 "넘어서는 것"이 아니라 **TIPS의 검증된 구조를 우리 물리 여건 (광고·강남 + 제3센터 남대문/IDC + 대전 DR)으로 충실히 재현하는 것이다.** 이것이 더 정직하고 방어 가능한 목표 설정이다. (국내 자체 PoC가 같은 구조로 15,000 TPS·자동복구를 확인한 것도 이 방향의 타당성을 뒷받침한다 — 단 그 PoC는 한은·참가기관 구간·인메모리 무장애·2센터 범위의 부분 실증이므로, 인메모리 장애 복원·순서 정확성·3센터 확장은 별도 실증(BMT)이 필요하다.)

5. 종합 — 대응방안 우선순위·이행 시사점

5.1 대응방안 우선순위

순위	이슈	핵심 대응	근거
1	① 무중단 복원력	근거리 3센터 A-A-A + 저널 순차처리 + 정족수 자동	RTO≈0·평판 = 최우선
2	③ 원장 정합성	전역 단일 순번·강한 일관성·도구 역할 분리(원장 동기화 금지)	이중지급·순서변경 = 절대 금기
★	3센터 정합성 검증	결정론적 재생·역등성·정족수 3중 방어(전제·한계 4건 관리)	이중지급 불가 논증 (2.3-부속)
3	② 고성능·확장성	현행 피크 기준선 + 수평 확장(실증 15,000 TPS)	전국민·스파이크
4	④ 전문 분산처리	메시지 큐 입구·순번기·역등성	폭주·중복·순서
★	참가기관 접속	대표 접속(⑦ 계승)·경로별 분담(결제=MQ 페일오버/API=GSLB)·행동규약·적합성 인증 — 성능 조건부(BMT)	참가기관 부담 최소·투명 전환(2.5)
★	기술 스택 구성	계층별 도구 배치(2.7)·핵심 코어 내재화	만능도구 아닌 역할별
★	신기술 평가	경로별 적용(인메모리·RDB-API·클라우드), 톤 조절·PoC·局간 공감대	신기술 과대포장 경계
5	⑤ 마감 없는 무결성	상시 대사·오염 탐지 3겹·짧은 체크포인트·저널 복제	24/365 특성
6	⑥ 유동성 관리	사전예치·유동성 절감(정책 병행 트랙)	참가기관 부담

순위	이슈	핵심 대응	근거
7	⑦ 무중단 운영	무중단 배포(카나리·Feature Flag 등)·야간 자동대응	멈추지 않는 운영

5.2 다른 과제와의 연계 (계승 관계)

본 과제는 기존 검토 결론 위에서 이어진다.

- **과제 ②(복원력)**: 펜싱+정족수 2/3, "결정 사람·실행 자동", 동기쌍+비동기 DR, 오염 탐지 3겹 → **그대로 계승·강화**(⑧은 "결정도 자동"으로 한 발 더). **스토리지**가 아닌 **저널(애플리케이션) 복제** 논거(3.1)도 ②와 직결.
- **과제 ⑤(MSA)**: "거액결제 독립 분리 = 최종 목표, Active-Active는 그 선결조건" → ⑧은 **소액 영역에서 다중센터 AA를 먼저 실현해보는 시험대**가 될 수 있다. 또한 RTGS 구축에 앞서 **비즈니스 단순화**를 위해 **회계결제시스템으로부터 한은금융망을 분리**하는 방향은 ⑤의 결합도 완화·독립 분리 논의와 직결되므로, **금융결제국·IT전략국 간 협의 재개**가 필요하다(2.6절 거버넌스와 연결).
- **과제 ⑦(연계환경)**: 대표주소+GSLB 자동전환 = FedNow의 단일접속 사상 → **재사용**(2.5 참가기관 접속·2.7 ① 계층).
- **과제 ⑩(인프라 자동화)**: 야간·주말 운영 자동화, 관측성·IaC·무중단 배포 → **계승**(2.7·3.3).
- **과제 ⑨(네트워크)**: 근거리 3센터 간 초저지연 전용망(다크파이버/DWDM + 백업회선·복수 통신사 이원화)은 ⑧의 동기복제 지연을 좌우하는 전제 → ⑨ **통신 효율화와 연계 검토**.

★ **스코프 경계(재확인)**: 위 근거리 제3센터(남대문/IDC)와 소액 RTGS 전용 인프라는 **과제 ⑧에만** 해당한다. 트랙 A(①②⑦)의 3센터 구성(광고·강남·대전)에는 확산·반영하지 않는다.

5.3 이행 시사점 — 2028년 전후 가동을 위한 관문

기술 설계가 옳아도, 이행은 **기술 하나만으로 완성되지 않는다**. 아래 다섯 가지는 시스템 구축과 **동시에 착수해야** 목표 시점(2028년 전후)이 성립하는 이행 관점의 핵심 시사점이다.

시사점	내용	성격
① 임계경로 = 제3센터	근거리 3센터 A-A-A(RTO≈0)의 전제인 제3센터(남대문 자체구축/IDC 임차)의 조성 기간이 전체 일정을 좌우 한다. 전산센터급 공간·전력·냉방·통신관로 확보는 리드타임이 길다.	인프라·일정
② 단계적 개시 옵션	제3센터가 늦어질 경우: (a) 수도권 IDC로 3센터를 선행 가동 후 남대문 완공 시 이전, 또는 (b) 2센터 + 정족수 전용 경량 거점으로 잠정 개시 (이 기간 복원력은 완성형보다 낮음을 명시). "완성형을 기다리다 전체가 지연"되는 것을 피한다.	이행 전략
③ 현행망과의 병행 운영	현행 공동망과 상당기간 병행 운영 → 참가기관·거래유형별 단계 이관. 빅뱅 전환은 24/365 인프라에 부적합. 상세는 아래 소절 .	이행 전략

시사점	내용	성격
④ 제도·법제 병행 트랙	결제 완결성 법제 — 은행이 도산해도 이미 끝난 결제를 되돌릴 수 없게 법으로 못박는 것 (국제기준 PFMI 원칙 1·8: 지급결제제도 지정·도산 시 완결성 보호). 여기에 비은행 애그리게이터의 참가·유동성 접근 근거 (한은법·규정), 24/365 원격관리 법적 제약 (국정원)까지 — 모두 기술이 아니라 정책·법제 사안 → 기술과 동시 착수 해야 가동 시점에 맞는다.	정책·법제
⑤ 거버넌스·조직·역량	소프트웨어 AA의 필연적 처리시간 지연에 대한 IT전략국·금융결제국 간 공감대 (허용 처리시간 합의), 운영기관 간 역할 재편(현행 운영기관 배제가 아닌 협력 모델), 코어(순번기·원장 엔진) 자체 개발·24/365 운영 조직 확보 (TIPS도 중앙은행 전담 개발조직이 구축·운영).	거버넌스·조직

③ 현행망과의 병행 운영 — SPOF 해소의 이행 수단 (핵심)

현행 전자금융공동망을 한 번에 대체(빅뱅 전환)하는 것은 24/365 국민 필수 인프라에서 감당하기 어려운 위험이다. 따라서 **신 소액 RTGS 가동 후에도 현행 공동망과 상당기간 병행 운영**하는 것을 기본 방향으로 한다. 이는 1.2절의 SPOF 해소 논리를 **실제로 구현하는 이행 전략**이다 — 두 시스템이 서로의 대비책이 되므로, 어느 한 시스템에도 전 국민 이체를 몰아넣지 않는다.

병행 운영의 축	내용
왜 병행인가	신 시스템 초기 안정화 리스크를 현행망이 백업(fallback)하고, 현행망 장애 시 신 시스템이 우회로가 됨 → 상호 이중화 = SPOF 해소의 실현
이관 방식	빅뱅 금지. 참가기관별·거래유형별 단계 이관 (선도 참가기관·저위험 거래부터 신 시스템으로 옮기고 관찰 → 확대)
존치 기간·판단 기준	현행망 존치 기간과 최종 이관(또는 영구 병행) 여부는 신 시스템의 안정성·이관율·리스크 지표로 판단 — 일정 못박기보다 지표 기반 단계 전진
이중 유입 방지	같은 이체가 두 망에 동시 유입되지 않도록 경로 배정 규칙 을 참가기관 규약에 명시(한 거래는 한 망으로). 경계 거래는 고유번호·역등성(2.4) 으로 중복 흡수
완결성 경계	두 망은 완결(finality) 기준이 다르다 (현행 DNS = 익일 차액정산 / 신규 RTGS = 건별 즉시). 병행기에는 어느 망을 거친 거래인지에 따라 완결 시점이 다름 을 참가기관·규정에 분명히 하고, 대사도 망별로 수행. (1.4·2.3-부속의 "완결 = 과반 센터 순번 확정" 정의는 신 RTGS를 경유한 거래에 한한다 — 현행망 경유 거래는 현행 DNS 규칙을 따른다.)
운영기관 관계	SPOF 해소가 특정 기관(금융결제원)의 배제를 뜻하지 않는다 . 병행기 현행망 운영·단계 이관·간접참가 게이트웨이 등에서 협력 거버넌스 를 설계(⑤와 연결)

요컨대 병행 운영은 "임시방편"이 아니라 **SPOF 해소를 안전하게 달성하기 위한 정공법**이다. 관건은 병행기의 **이중 유입 방지·망별 완결성 구분·지표 기반 이관 판단**이며, 이는 기술 설계와 제도(참가규약·완결성 법제)가 함께 정해야 한다(6.1).

한 줄 결론: "구조는 정해졌고, 남은 것은 성립 조건(제3센터·BMT)과 제도(법제·거버넌스)의 병행 착수 — 그리고 현행망과의 상당기간 병행 운영을 통한 안전한 이행이다." 기술·인프라·제도의 세 트랙이 같은 일정선 위에서 함께 가야 2028년 전후 가동이 현실이 된다. 각 항목의 구체 실측·검증 방법은 6장에서 다룬다.

6. 향후 추가 검토 고려 사항

6.1 확인 필요 (정량화·결정 관문)

대응방안을 정밀 설계하려면 다음 측정·결정이 선행되어야 한다. (일부는 이미 방향이 정해졌다.)

항목	현황	설계 영향
1. 현행 실측 피크 TPS	약 2,000 TPS 미만 (기준선 확보)	목표는 이를 기준선으로 한 확장성 (scalable) — 절대치보다 증설 용이성
2. 제3센터 확보 방식	1순위 남대문 본점 자체구축 / 2순위 수도권 IDC	근거리 3센터 A-A-A(RTO≈0)의 필수 전제 — ⑧ 전용(이슈①)
3. 남대문 본점 여건	세 구간(광고·강남·남대문) 실측 왕복지연·전산센터급 공간/전력/냉방·급전·통신관로 물리 분리	동기복제 성립 여부·구축 타당성(이슈①)
3-1. 대전 DR 비동기 지연	남대문-대전 실측 왕복지연·평상시 비동기 복제 lag	광역재해 시 손실 범위(RPO) 산정 (이슈①·5.3③)
4. 교차거래 비율	실측 어려움 (저널 순차처리는 무관하게 성립)	샤딩 최적화 옵션 채택 여부의 판단 변수(이슈①)
5. 단일 순번기 처리량 한계	PoC/BMT 실측 필요 (기존 실증 15,000 TPS는 무장애 전제)	코어 병목 상한·확장 설계(2.3-부속·2.7)
5-1. 인메모리 코어 장애 복원	BMT 필수 (기존 PoC 무장애 전제라 미검증)	선저널(write-ahead) 무손실 승계 실증 — 부록 A S2는 모델 검증
5-2. 순서 오류율·교정 지연	BMT 측정 필요 (드문 순서오류 실측)	탐지·교정 장치 성능·잔류 불일치율(2.3-부속·부록 A S4)
5-3. 규정 조회 기준순번 규율	설계·규정 확정 필요	지급준비금·마감 잔액을 "기준 순번 (sequence point)"으로 고정, 1차 기준센터·정족수 승계 규칙(2.3-부속 위험4)

항목	현황	설계 영향
6. 사전예치·일중당좌대출	예치= 참가기관 자율, 일중당좌대출 이용 가능	24/365(야간·주말) 운영 방식만 추가 검토(이슈⑥)
7. 체크포인트(시점 복구) 주기	추후 결정	마감 없는 시스템의 복구 정밀도(이슈⑤)
8. 원장 DB 솔루션 성숙도	PoC/BMT 검증 필요 (상용·국산·오픈소스)	원장 DB 채택 — 24/365 무중단·무손실 검증(2.6·2.7)
9. 局간 처리시간 공감대(거버넌스)	PoC 후 협의 필요	소프트웨어 AA의 필연적 지연을 측정해 IT전략국·금융결제국 합의(2.6)
10. 한은금융망 분리 검토 재개	금융결제국·IT전략국 협의 대상	비즈니스 단순화·복잡도 완화 — 과제 ⑤와 직결(2.6·5.2)
11. 24/365 원격관리 법·제도 제약	국정원 원격관리 불허 등 확인 필요	무인·원격 운영 가능 범위 → 이슈⑦ 운영 설계 전제
12. 참가 구성·애그리게이터 제도	정책 결정 필요 (직접 참가 범위·간접 참가 경유 방식·전용계좌 수)	접속 규격·적합성 인증 대상·유동성 규모 (2.5·이슈⑥) — 금융결제국 협의
13. 접속 전환 성능 (MQ 페일오버·GSLB)	BMT 측정 필요 (처리시간 오버헤드·전환 시간·재접속 폭주 — 결제=MQ 클러스터 페일오버 / API=GSLB)	경로별 대표 접속 본안(A) 채택 조건 — 미달 시 복수 주소 방식(2.5·6.4)
14. 결제 완결성 법적 기반	법제 정비 필요 (지급결제제도 지정, 도산 시 완결성 보호, 비은행 직접 참가·유동성 접근의 법적 근거)	24/365 완결성과 비은행 참가의 전제 (PFMI 원칙 1.8) — 시스템 가동 전 완비 필수(1.4·3.2)
15. 비용·대안 개산 비교	개산 필요 (남대문 자체구축 vs IDC 임차, 24/365 교대 인력 소요, 축소 대안 대비 효익)	투자 의사결정 근거 — 2.1 트레이드오프의 정량화
16. 현행망 병행 운영 설계	설계·협의 필요 (이중 유입 방지 경로배정 규칙, 망별 완결성 구분, 현행망 존치 기간·지표 기반 이관 판단, 금융결제원 협력 거버넌스)	상당기간 병행 운영 = SPOF 해소 이행 수단(5.3-③) — 금융결제국·금융결제원 협의

→ 핵심 설계(근거리 3센터 A-A-A + 저널 순차처리 + 정족수 자동)는 국제 실증(TIPS)·한은 자체 PoC로 타당성이 확인된 구조다. 위 변수들은 **정밀화·최적화(제3센터 확정, 순번기 한계, 처리시간 합의) 단계의 과제**다.

6.2 중장기 검토 과제

1. **거액결제와의 관계 — 소액이 거액 AA의 시험대:** 소액 RTGS는 건별 독립이라 다중센터 A-A-A가 자연스럽게 성립한다(거액의 "다자간 동시처리 = 못 쏘갠"과 정반대). 소액에서 저널 순차처리·정족수 자동전환을 먼저 구현하면 역량·도구가 축적된다. 다만 **거액결제 독립 AA 자체는 향후 10년 내 도입 대상이 아니며**, 미국·유럽·호주 등 주요국 거액 RTGS도 계정계 코어는 AA로 운영하지 않는다.
2. **유동성 절감 정책 트랙:** 사전예치·일중당좌대출의 24/365(야간·주말) 운영 방식은 기술이 아니라 정책·제도 결정 사항 → 별도 병행 트랙으로 검토(이슈⑥).
3. **핵심 코어 기술 내재화:** 순번기·원장 엔진 등 가장 특수한 코어는 자체 개발로 내재화하고, 주변부는 검증된 오픈소스·상용을 혼합(2.7). 내재화의 **실행 모델(자체 개발/공동 개발/외주 후 단계 이관)**을 비교 선택하고, 코어 개발·24/365 운영 조직의 확보 계획을 함께 수립한다(TIPS도 중앙은행 전담 개발조직이 구축·운영). 24/365 무중단 배포 역량도 과제 ⑩ 과 연동해 축적. (조직·역량 확보는 5.3- ⑤ 이행 시사점과 직결.)

이행 일정·단계적 개시·현행망 이관·법제·거버넌스 등 **이행 관점의 시사점은 5.3에 총괄했다**. 6장의 확인필요(6.1)·BMT(6.4)는 그 시사점들을 실측·검증으로 뒷받침하는 관문이다.

6.3 다음 단계

1. **제3센터 확정** — 남대문 본점 여건(공간·전력·거리 지연) 조사 → 자체구축/IDC 결정.
2. 현행 피크 TPS·단일 순번기 처리량 한계 PoC → 확장 목표 확정.
3. 도구 역할 분리(입구 메시지 큐·강한일관성 원장·조회 사본) 및 근거리 **3센터** 정합성·자동복구 PoC — 이중지급·순서변경 방지 실증(한은 2센터 실증의 3센터 확장).
4. 24/365 무중단 배포·야간 자동대응 운영 체계 설계(②⑩ 통합).
5. **차기 BMT 설계** — 아래 6.4의 중점 검증 항목을 시험 계획으로 구체화.

6.4 차기 BMT(실증시험) 중점 검증 항목 (제안)

기존 PoC가 확인한 것(한은-참가기관 구간 15,000 TPS·2센터 정합성·자동복구)과 확인하지 못한 것을 가른 뒤, **미검증 급소를 정조준**한다. 합격 기준은 안(案)이며, 처리시간 관련 기준은 局간 협의(6.1-9)로 확정한다.

#	검증 항목	무엇을 재는가	합격 기준(안)	미달 시 대응
1	순번기 처리량 상한	3센터 동기 합의를 포함한 전역 순번 부여의 상한 TPS	현행 피크(2,000)의 충분한 여유 배수 확보 + 병렬 구간의 선형 확장 확인(직렬 코어는 상한 자체를 실측)	경량 명령문 축소·코어 최적화, 최후엔 샤딩 옵션 재검토(2.1)
2	3센터 합의 지연	광교-강남-남대문 실측 왕복 + 부하 상태의 거래당 합의 지연(p99)	평시 수 ms, 피크에도 목표 처리시간 이내	제3센터 후보지 재검토(IDC, 전용망 증강(⑨ 연계))
3	인메모리 코어 장애 승계	처리 도중 코어 강제 종료 → 선저널(write-ahead) 무손실 승계	유실 0·이중지급 0·승계 수 초 이내	선저널 규율 강화·체크포인트 주기

#	검증 항목	무엇을 재는가	합격 기준(안)	미달 시 대응
				단축(부록 A S2의 실물 재현)
4	순서오류율·교정 지연	실부하에서 순번 gap·역전 발생률과 보류(pending) 재정렬 소요	잔류 불일치 0(상시 대사 100% 포착)·교정 지연 수십 ms 이내	저널 적용 경로의 직렬화 강도 상향(2.3-부속)
5	접속 전환(MQ 페일오버·GSLB)	센터 상실 시 재접속 시간·재전송 폭주 흡수·평시 처리시간 오버헤드 — 결제 경로는 MQ 클러스터 페일오버, API 경로는 GSLB 각각 측정	오버헤드가 처리시간에 유의미하지 않음·재접속 수 초·유실 0	대안 B(복수 주소 명시)로 전환(2.5)
6	스파이크 완충	순번기 상한 초과 부하에서 입구 큐 적체·소진·유실	유실 0·적체 수 초 내 소진(부록 A S5의 실물 재현)	입구 증설·유입 제어(백프레서) 설계 추가
7	원장 DB 페일오버	후보 DB(상용·국산·오픈소스)의 동기복제 + 자동 페일오버 반복 시험	페일오버 무손실·연속 반복에도 안정	운영 성숙도 높은 상용 DB 우선(2.6)
8	end-to-end 처리시간	참가기관 구간을 모사하고 응답·완결 규율(과반 확정 후 응답)을 적용한 상태 의 고객 체감 1건 처리시간	局간 합의 목표치(참고: TIPS 규정 5초·실측 초 미만)	처리시간 목표 재협의를(거버넌스, 6.1-9)

1~4는 본 아키텍처의 성립 조건이다 — 미달 시 설계 자체를 수정한다. 5~8은 품질·채택 조건이다 — 미달 시 대안 전환·목표 조정으로 흡수한다.

맺음말

본 검토의 결론은 세 층으로 요약된다. 첫째, **구조는 정해졌다**. 근거리 3센터 A-A-A + 저널 순차처리 + 정족수 자동전환은 유럽 TIPS가 실증(RTO=0)하고 국내 PoC와 모의 시뮬레이션(부록 A)이 뒷받침하는, 방어 가능한 골격이다. 둘째, **성립 조건이 남았다**. 제3센터(남대문)의 물리 여건과 순번기 처리량·합의 지연의 실측이 이 골격의 전제이며, 6.4의 BMT 항목 1~4가 그 관문이다. 셋째, **제도가 병행되어야 한다**. 참가 구성(직접·간접), 비은행 참가자의 유동성 접근, **결제 완결성의 법적 기반(PFMI 원칙 1-8)**, 처리시간 목표의 局간 합의는 기술이 아니라 정책·법제의 영역이며, 기술 일정과 동시에 착수해야 전체 일정이 성립한다.

부록 A. 모의 시뮬레이션 검증 결과

본 아키텍처의 핵심 주장(무중단·정합성)을 논리에만 맡기지 않고, **간이 모델을 코드로 작성해 직접 실행·검증**했다. 아래는 그 요약이다. (개념 검증용 단순 모델이며 성능 수치의 확정이 아니다 — 물리 지연은 근사 모사이고, 실거래의 보안·예외처리 부하와 고객단 end-to-end는 미포함. 실제 성능은 BMT의 몫이다.)

검증 목적

특히 **국내 PoC가 다루지 못한 영역**을 겨냥했다: ① 인메모리 코어 장애 시 무손실 승계 ② 드물게 발생하는 순서 오류의 실제 피해와 교정 효과. (PoC는 인메모리 무장애·한은-참가기관 구간·2센터 전제였다.)

시나리오별 결과

시나리오	무엇을 확인했나	결과
S1 평상시	3센터가 같은 저널을 재생 → 잔액 일치	3센터 완전 일치 , 총액 보존, 이중지급 0, 합의지연 유사 수 ms
S2 인메모리 장애	코어 1개 강제 종료 → 선저널 (write-ahead) 승계	생존 2센터 무중단, 재기동 센터가 저널 재생으로 100% 복구 , 유실 0
S3 split-brain	망 분할 시 소수측 펜싱 → 이중처리 차단	소수측 정지 , 과반측 지속, 이중지급 0
S4 순서 오류	순서 뒤섞임 주입 → 탐지·교정 효과	교정 없으면 의존 거래 오거절 1,300여 건 , 교정 켜면 정답과 동일 (오거절 최소)
S5 스파이크	순간 폭주 → 입구 큐 완충	순번기 상한 이내면 적체 0, 초과해도 큐가 버터 유실 0 ·수 초 내 소진

시사점

- **S2·S4가 핵심 수확이다.** 인메모리 장애 무손실 승계(S2)와 순서 오류의 교정 흡수(S4)는 모두 국내 PoC의 사각지대였는데, **선저널 규율과 탐지·교정 장치로 해결됨을 코드로 확인**했다.
- 특히 S4는 **"순서 오류는 원천 불가능"이 아니라 "탐지·교정으로 흡수하는 문제"**라는 본 보고서(2.3-부속)의 서술을 정량으로 뒷받침한다.
- 다만 이는 모델 검증이므로, **실물 성능·순서오류율·인메모리 승계 시간은 BMT로 실측**해야 한다(6.1의 확인 필요 항목).

시뮬레이션 코드·시나리오·원자료는 프로젝트 작업 폴더([reports/8/sim/](#))에 결정론적 재현 형태로 보존한다.

본 보고서의 아키텍처는 제안 수준의 설계 방향이며, 위 확인 필요 항목의 실측·협의 결과에 따라 정밀화한다.