OPENMARU

PREVENTIVE INSPECTION INTELLIGENCE

공공 정보시스템 예방점검 지능화

고시 제2026-23호 의무화에 대응하는 OS·미들웨어·DBMS 판정·증적·운영 지식 축적 방안

대상	DATE
공공기관 정보화 부서	2026.11



CONFIDENTIAL

예방점검 의무화 대응 순서

KEY INSIGHT 예방점검의 산출물이 점검표에서 판정 근거·승인·재점검 기록으로 바뀜 — 차년도 요구사항도 이 기록을 기준으로 정함

01 **2026 예방점검 의무화로 바뀐 기관 의무**
등급 재분류·안정성 고시·3개 분야 점검

02 **판정 근거 없는 점검표의 감사 리스크**
2023년 장애 사례·단순 자동화의 빈칸

03 **단순 자동화와 지능화의 차이**
수집부터 학습까지 6단계 비교

04 **예방점검 솔루션 아키텍처**
APM·OpsKnow Agent·OpsKnow 역할

05 **AAS 위 OpsKnow Agent의 통제 구조**
결정적 코드 판정·승인 코드·작업 경계

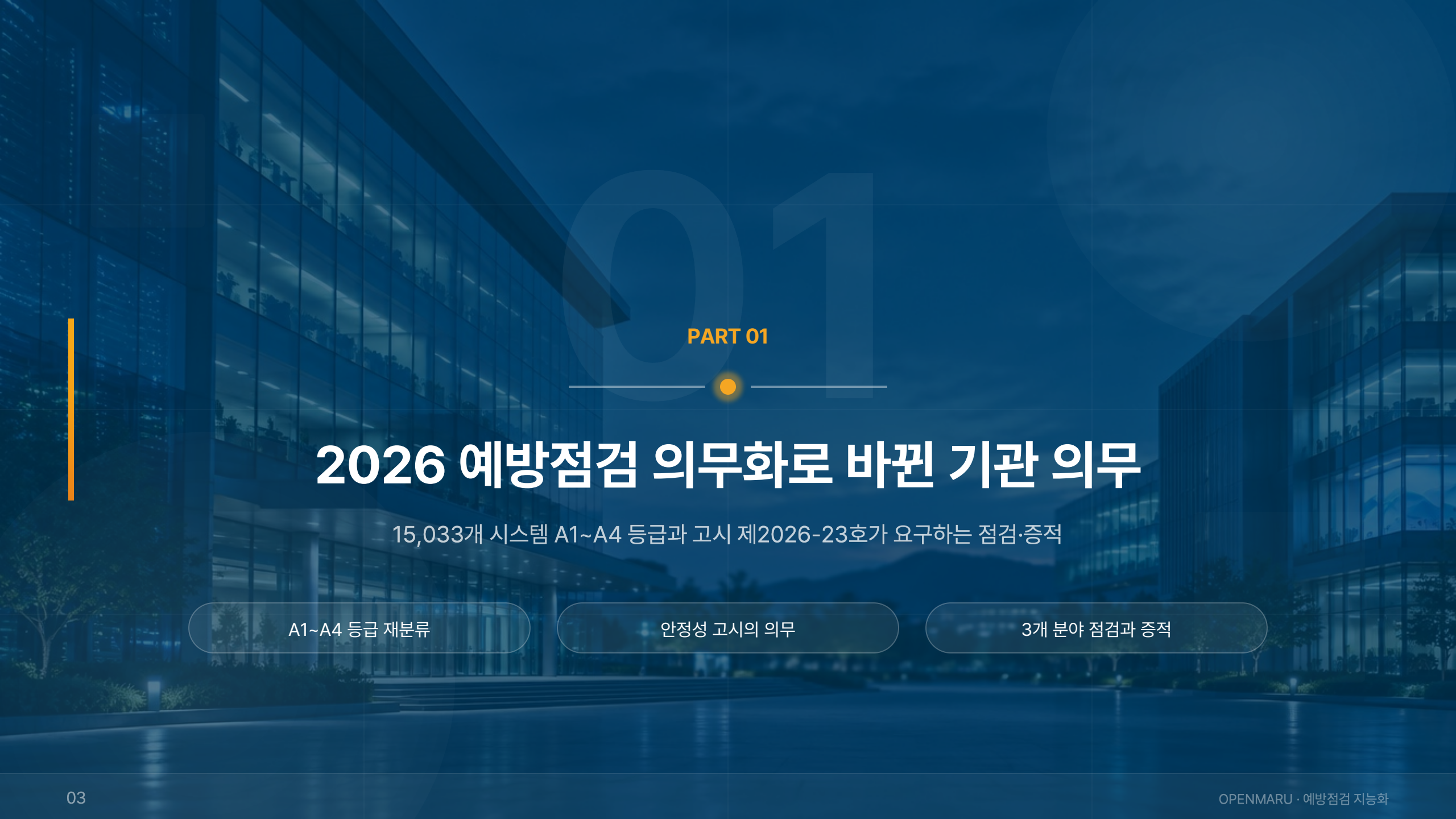
06 **소버린 AI Level 3 폐쇄망 운영**
외부 송신 0건·GPU 1대 30B sLLM

07 **보안 취약점 점검의 지능화**
KISA·CVE 권고부터 재점검까지

08 **OpsKnow 운영 기록 통합과 결재 경계**
Incident·점검 결과·정기 보고

09 **관리자 사용 장면과 응답 예시**
자연어 요청 네 가지 장면

10 **경쟁 방식 비교와 차년도 사업 준비**
측정 지표·요구사항·RFP 문안



PART 01

2026 예방점검 의무화로 바뀐 기관 의무

15,033개 시스템 A1~A4 등급과 고시 제2026-23호가 요구하는 점검·증적

- A1~A4 등급 재분류
- 안정성 고시의 의무
- 3개 분야 점검과 증적

등급별 시스템 분포와 목표복구시간

KEY INSIGHT A1·A2 230개는 복구 속도가, A4 14,132개는 점검 물량이 과제 — 등급별로 점검 체계의 설계 기준이 다름

공공 정보시스템 15,033개의 등급별 분포

2026-08-27 행정안전부 발표 · 국민 서비스 중요도 기준



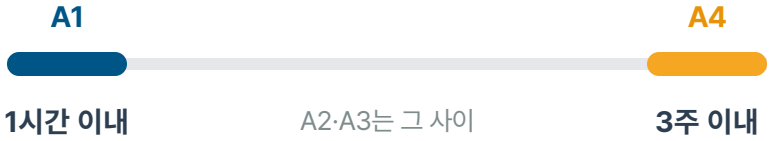
A1+A2 230개(1.5%)만 가장 엄격한 복구 목표 적용

등급 기준의 변화

이전 기준	2026년 기준
기관 규모·사용자 수	국민 서비스 중요도

계기: 2025년 9월 국가정보자원관리원 화재 때 사용자 수가 적어 낮은 등급을 받은 핵심 시스템 문제

등급별 목표복구시간(RTO)



상위 등급은 판정 속도와 정확성, 하위 등급은 판정 규모와 일관성이 점검 체계의 기준

Source: 행정안전부 보도자료(2026-08-27), 디지털데일리(2026) · 목표복구시간은 행정예고안 보도 기준

안정성 고시의 기관 의무

KEY INSIGHT 예방점검이 권고에서 감사 대상 의무로 바뀜 — 위탁 운영·민간 클라우드 계약에도 같은 기준이 들어가야 함



안정성 기준 46개

예방점검·장애 관리를 포함한 최소 조건 목록

표준운영절차·SLA

민간 클라우드와 위탁 운영 계약까지 SLA 체결

실전환 훈련

연 1회 이상 대체 환경으로 실제 전환

장애관리 계획

3년 기본계획 + 해마다 연간 시행계획

백업 의무

모든 시스템에 주기 백업·원거리 소산 백업

장애 즉시 보고

중요 시스템 장애는 디지털안전상황실에 즉시

Source: 보안뉴스(2026) "정보시스템 안정성 고시" 제정 · 행정예고안(2026-03) 보도 기준

점검 분야별 주기와 연간 판정 건수

KEY INSIGHT 판정 건수는 일상점검과 A4 시스템에서 크게 늘어남 — 사람 손 없이 판정과 기록을 남겨야 할 범위가 여기서 정해짐

분야	보는 대상	빈도와 깊이	주요 대상 영역
일상점검	CPU·메모리·디스크, 메인 화면 접속·응답 시간, 인증서·도메인 만료	매일 · 얕고 넓게	OS · 웹 서버 · WAS · DBMS
특별점검	성능 중심의 심화 항목	주기적 · 깊게	OS · WEB/WAS · DBMS
구조진단	시스템 구성 전반이 장애에 견디는 구조인지	장기 주기 · 구조 전체	시스템 아키텍처

연간 판정 건수 산식

대상 장비 수 (기관 입력) × **영역별 항목 수** (기관 점검표 기준) × **연간 수행 횟수** (일상점검은 업무일 수) = **판정 건수** (3개 분야 합계)

늘어나는 쪽

일상점검은 수행 횟수가 업무일 수만큼 커지고, 시스템의 94.0%가 A4라 판정 건수 대부분이 하위 등급에서 나옴

계산 결과의 쓰임

인력 증원 규모보다 판정과 기록을 사람 손 없이 남겨야 하는 범위를 정하는 근거

Source: 행정안전부 정보시스템 예방점검체계(2024-10) · 3개 분야 8개 점검항목

감사가 확인하는 증적 요소

KEY INSIGHT 판정·조치·재점검이 서로 다른 도구에 흩어지면 담당자 기억으로 이어 붙이게 됨 — 같은 기록 번호로 묶어야 한 번에 조회됨

01

판정 근거

담는 내용

지표 값 · 기준값 · 판정 시각

빠지면 생기는 문제

정상 판정의 근거를 설명하지 못함

02

조치 이력

담는 내용

승인자 · 조치 내용 · 실행 시각

빠지면 생기는 문제

이상 판정 뒤 처리 여부를 입증하지 못함

03

재점검 결과

담는 내용

조치 뒤 같은 항목의 판정

빠지면 생기는 문제

조치가 효과가 있었는지 알 수 없음

예산 요구서에 나눠 적을 두 묶음

자동 판정으로 넘기는 항목

값을 모으기만 하면 판정할 수 있는 항목 → 수집 도구와 판정 코드

사람 확인으로 남는 항목

사람이 판단해야 하는 항목만 인력 산정에 포함

Source: 고시 제2026-23호 행정예고안 · OPENMARU 증적 요소 분석 · 2023-11-25 정부 발표(행정전산망 장애 원인)

PART 02

판정 근거 없는 점검표의 감사 리스크

체계가 없을 때와 단순 자동화만 했을 때 비어 있는 기록

2023년 행정전산망 장애

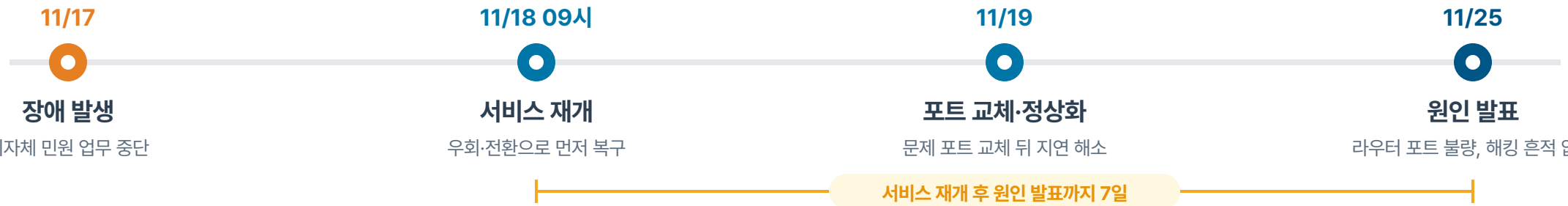
단순 자동화의 빈칸

감사 질문 자가진단

행정전산망 장애의 복구와 원인 발표 시차

KEY INSIGHT 복구보다 원인 설명이 늦었음 — 장비별 점검 이력이 쌓여 있으면 원인 후보를 좁히는 시간이 줄어듦

2023년 11월 지방행정전산서비스 장애 경과 (정부 발표 기준)



원인 지목의 변화

시점	지목된 원인	근거
장애 직후	L4 스위치 OS 업데이트 오류	초기 보도
11/25 발표	라우터 포트 불량, 해킹 흔적 없음	정부 브리핑
발표 이후	근본 원인에 대한 다른 시각	언론 보도

평소 점검표에 있어야 할 수명 주기 항목 (예시)

- **도입 시점·내구연한** — 자산 대장 갱신일, 교체 계획 문서
- **펌웨어·OS 버전** — 지원 종료 여부, 수정본 적용 기록
- **포트·인터페이스 오류** — 날짜별 오류 카운터와 판정 결과
- **이중화 경로 전환** — 전환 시험 일시와 결과

Source: 뉴시스(2023-11-25), 디지털데일리(2023-11-26) · 정부 발표 기준 경과

단순 자동화는 판정 근거를 남기지 못함

KEY INSIGHT 스크립트는 값을 비교할 뿐 해석하지 못함 — 임계치 초과 표시 한 줄로는 감사 질문에 답할 수 없음

자동화 층 — 단순 자동화가 채우는 범위

매일 수집 → 임계치 비교 → 양식 칸 채움 → 날짜별 보관

증적 층 — 감사가 요구하지만 비어 있는 세 칸

판정 근거

남는 것
임계치 초과 여부 표시

감사·장애 분석이 요구하는 것
어떤 기준과 이력으로 정상·이상을 판단했는지

영역 간 연관

남는 것
OS·미들웨어·DBMS 항목별 개별 결과

감사·장애 분석이 요구하는 것
한 영역의 이상이 다른 영역 어느 지표와 함께 움직였는지

조치와 재점검

남는 것
다음 날 점검 결과

감사·장애 분석이 요구하는 것
누가 승인해 무엇을 조치했고 재점검 결과가 무엇인지

결과: 점검표에는 "이상" 칸만 남고, 판정 근거·영역 연관·승인과 재점검은 담당자 기억과 별도 문서로 흩어짐

Source: 행정안전부 예방점검체계 일상점검 항목 · OPENMARU 분석(단순 자동화 산출물과 감사 요구 대조)

분기 보고와 SLA 산출의 수작업 비용

KEY INSIGHT 상위 보고서가 원자료가 아닌 하위 보고서를 다시 요약함 — 담당자가 바뀌면 수치 근거를 되짚을 길이 끊김

보고 주기별 수작업 단계

일일

- 수작업: **이상 표시 항목 확인, 조치 필요 여부 메모**
- 근거 위치: 점검표 파일, 메신저 대화

▼

주간·월간

- 수작업: **이상 항목 발췌, 장애 기록·조치 내역 대조, 차트 캡처**
- 근거 위치: ITSM 도구, 결재 문서, 모니터링 화면

▼

분기·연간

- 수작업: **하위 보고서 취합, SLA 준수율 계산, 양식 편집**
- 근거 위치: 엑셀 집계표, 위탁 운영사 보고서

SLA 산출에서 받는 감사 지적 유형

1. **장애 시작 시각이 문서마다 다름**
   질문: 어느 시각을 썼고 근거 기록은 무엇인가
2. **계획 정지 제외 근거 부족**
   질문: 제외한 정지가 사전 승인 작업이었다는 기록이 있는가
3. **위탁사 보고와 기관 측정값 불일치**
   질문: 두 값이 다른 이유와 최종 값을 정한 근거는 무엇인가
4. **재계산 불가**
   질문: 같은 원자료로 같은 준수율을 다시 산출할 수 있는가

Source: 고시 제2026-23호 행정예고안(SLA 체결 의무, 민간 클라우드·위탁 운영 포함) · OPENMARU 분석

예방점검 수준 자가진단

KEY INSIGHT 승인 기록 문항이 단순 자동화와 지능화를 가르는 경우가 많음 — 단순 자동화 단계는 수집 확대보다 판정 근거·승인 기록이 먼저임

감사에서 받는 5가지 질문

1. **판정 근거**
   점검 결과의 판정 근거를 보여 줄 수 있는가 ☐
2. **승인 기록**
   조치마다 승인 기록이 있는가 ☐
3. **재점검 결과**
   조치 뒤 재점검 결과가 남는가 ☐
4. **이력 연결**
   장애 이력과 점검 이력이 연결되는가 ☐
5. **보고서 재생성**
   보고서가 원자료에서 다시 생성되는가 ☐

충족 문항 수로 보는 단계

0~1개
체계 없음

담당자별 수기 점검, 기록 형식 제각각

리스크·과제
원인 규명 지연

2~3개
단순 자동화

스크립트 수집·양식 보고, 승인·재점검은 별도 문서

리스크·과제
판정 근거·승인 기록 감사 지적

4~5개
지능화

판정·승인·재점검·보고가 한 저장소에서 이어짐

리스크·과제
판정 기준의 주기 검토

Source: OPENMARU 예방점검 자가진단 기준 · 감사 질문 5문항

PART 03

단순 자동화와 지능화의 차이

수집·판정·연관·조치·보고·학습 6단계에서 남는 산출물 비교

- 판정 근거를 남기는 코드
- 트랜잭션 연관 판정
- 조치에서 학습까지

세 수준의 차이는 판정부터 벌어짐

KEY INSIGHT 차년도 투자는 판정 규칙을 코드로 옮기고 승인 기록을 붙이는 쪽에 둬야 함 — 수집 확대만으로는 지능화 단계에 닿지 않음

운영 단계	체계 없음	단순 자동화	AI 지능화
수집	담당자가 접속해 수기 점검표에 기록	스크립트가 주기적으로 수치를 파일로 저장	**APM 트랜잭션 단위 지표 추가, 원자료 보존**
판정	경험으로 판단, 근거 없음	임계치 초과 여부만 표시	**결정적 코드가 입력 값·적용 규칙·상태를 함께 기록**
연관	영역별 담당자가 따로 확인	OS·WAS·DBMS 경보가 각각 발생	**트랜잭션 ID로 지표를 묶어 원인 후보 제시**
승인	구두·메신저	시스템 밖 결재 문서, 점검 결과와 분리	**1회용 승인 코드로 승인자·시각·대상을 점검 기록에 연결**
조치	직접 변경, 기록 누락 쉬움	스크립트 실행 가능하나 승인과 미연결	**승인 뒤 실행, 적용 직전 재확인, 적용 뒤 재점검**
보고	문서를 새로 작성	양식 칸 자동 채움	**원자료에서 재생성, AI가 설명문 작성**
학습	담당자 기억	보고서 파일 보관	**Incident 기록이 OpsKnow에 쌓여 다음 판정 근거로 조회**

차년도 요구사항 **판정 근거 · 승인 연결 · 원자료 보고 · 지식 축적**

Source: OPENMARU 예방점검 지능화 단계 비교

결정적 코드 판정과 판정 보류 원칙

KEY INSIGHT "확인하지 못함"과 "확인했고 정상"을 구분하는 것이 감사 재현성의 출발점 — 판정 보류가 늘면 수집 경로 문제의 신호임

단순 자동화의 판정

디스크 임계치 80% · 실측 78%

/data 정상

보고서에 남지 않는 것

- 임계치를 정한 시점과 결정자
- 지난주 값과 추세
- 다른 파일시스템 확인 여부
- "확인 못함"과 "정상"의 구분

결정적 코드 판정 기록

같은 입력에 늘 같은 판정 — 감사 때 다시 실행해 확인

상태	정상 · 주의 · 이상 · 판정 보류
대상	서버 이름, 점검 항목
시각	점검 시각, 값의 수집 시각
입력 값	원래 값 (예: 디스크 78%, 지난주 71%)
적용 규칙	기준값과 규칙 버전

판정 보류 원칙

확실하지 않으면 정상이나 최신으로 판정하지 않음 — 근거가 부족하면 판정 보류와 사유를 기록하고, 마지막 결과를 재사용하지 않음

정상 건수 집계 | 이상 건수 집계 | 판정 보류 건수 집계

보고서는 세 값을 따로 집계 · 보류가 늘면 수집 경로·저장소 연결 점검

Source: OPENMARU OpsKnow Agent 판정 설계

트랜잭션 ID로 묶는 계층 연관 판정

KEY INSIGHT 담당자가 받는 정보가 경보 세 건에서 근거 지표가 붙은 원인 후보 한 건으로 줄어듦 — 첫 확인 대상이 영역마다 갈리지 않음

가상 예: 민원 조회 서비스 응답 지연

단일 지표 경보

- **WAS** 스레드 사용률 경보
- **DBMS** 커넥션 풀 대기 경보
- **OS** CPU 사용률 경보

영역마다 첫 확인 대상이 다름

계층 연관 판정 — 같은 트랜잭션 ID로 묶은 원인 후보

SQL 수행 시간 증가 → **커넥션** 반환 지연 → **커넥션 풀** 고갈 → **WAS 스레드** 누적

첫 확인 대상: 수행 시간이 늘어난 SQL

연결 방식: APM이 요청마다 트랜잭션 ID를 붙여 WAS 스레드·DB 커넥션·SQL 수행 시간을 묶고, OS 자원은 서버 이름과 수집 시각으로 연결

비교 항목	단일 지표 경보	계층 연관 판정
Incident에 남는 원인	영역별 소견이 따로 남음	원인 후보와 관련 트랜잭션 ID

연관 판정은 후보까지 — 최종 원인은 조치 결과와 재점검으로 확인

Source: OPENMARU APM 트랜잭션 추적 · 가상 예시(민원 조회 서비스 응답 지연)

조치 이후 기록이 다음 판정으로 돌아옴

KEY INSIGHT 학습 효과는 판정 옆에 붙는 과거 근거가 늘어나는 데서 나옴 — 차이가 가장 오래 누적되는 단계임



조치 기록에 남는 순서

01 원래 점검 결과	02 판정 상태	03 승인자·승인 시각	04 승인 코드 사용
05 적용 직전 확인	06 적용 내용	07 재점검 결과	

비교	손으로 고친 보고서	원자료에서 재생성
숫자의 출처	스크립트 출력 위에 사람이 수정	**저장된 판정·조치 기록에서 계산**
같은 기간 재작성	수정 이력 없으면 재현 불가	**언제나 같은 숫자**
감사 대응	보고서와 원자료를 따로 맞춤	**숫자에서 원자료로 바로 이동**

Source: OPENMARU OpsKnow · OpsKnow Agent 조치 기록 구조





PART 04

예방점검 솔루션 아키텍처

수집·판정·저장·가시화를 다섯 구성요소가 나눠 맡는 예방점검 구조

APM 상시 수집

OpsKnow Agent 판정

OpsKnow 축적과 화면

예방점검 구성요소별 역할 분담

KEY INSIGHT 사람이 개입하는 자리는 수집 대상 등록, 조치 승인, 보고서 검토, 재발방지 입력으로 정해져 있음 — 나머지는 자동으로 이어짐

수집

OPENMARU APM

맡는 일
OS·미들웨어·DBMS 지표 상시 수집

산출물
시계열 지표, 트랜잭션 추적

사람이 하는 일
수집 대상 등록

판정

OpsKnow Agent

맡는 일
임계치 판정, 조치 제안, 보고서 초안

산출물
판정 결과, 조치안, 보고 초안

사람이 하는 일
조치 승인, 보고서 검토

저장

OpsKnow

맡는 일
판정·Incident·정기 보고 축적과 검색

산출물
점검 이력, 장애 기록, 운영 보고

사람이 하는 일
재발방지 내용 입력

가시화

Wallboard

맡는 일
운영실 상시 화면

산출물
시스템 상태, 점검 이행 현황

사람이 하는 일
이상 표시 확인

가시화

전국 Dashboard

맡는 일
다기관 통합 화면

산출물
등급별 시스템 현황, 미이행 점검

사람이 하는 일
상급 기관 보고 결재

CogentAI 근거 검색(RAG)과 30B 수준 내부 sLLM 서빙을 기관 서버 안에서 담당 — 판정·설명 단계의 AI 엔진

Source: OPENMARU APM · OpsKnow · OpsKnow Agent · CogentAI · Wallboard · 전국 Dashboard 구성

APM 수집 지표와 일상점검 항목 대응

KEY INSIGHT 점검 결과와 증적이 같은 원천에서 나오게 됨 — 비용은 수집 장치보다 판정 규칙과 보고 양식을 정하는 쪽에 듦

점검 영역	대표 점검 항목	OPENMARU APM 수집 지표	증적으로 남는 형태
OS	CPU·메모리·디스크 상태	**서버 자원 사용률 시계열**	점검 시각 값과 전후 추이
WEB/WAS	메인 화면 접속 여부와 접속 시간	**실제 요청의 응답 시간·오류율**	시간대별 응답 분포
WEB/WAS	성능 저하 원인	**JVM 힙, GC, 스레드, 느린 트랜잭션**	트랜잭션 ID별 추적 기록
DBMS	커넥션 상태	**WAS 쪽 커넥션 풀 사용률·대기**	시계열과 임계 초과 이력
DBMS	느린 SQL	**SQL 수행 시간·호출 빈도**	SQL별 상위 목록

증적 원천 세 갈래 — 같은 점검 회차 아래 출처 표시와 함께 보관

APM 기록으로 채움

WAS 응답·GC·스레드, 커넥션 풀, 느린 SQL, 서버 자원

→ 자동 판정 후 저장

사람 확인 후 입력

네트워크 장비 상태, 백업 실물, 이중화 전환 훈련

→ 확인 결과를 첨부로 저장

혼합

성능 저하 원인 규명, 재발방지 조치

→ 담당자가 재발방지 입력

Source: OPENMARU APM 수집 범위 · 영역별 항목 수는 공개 원문 대조 전이라 적지 않음

정기 점검의 자동 실행 순서

KEY INSIGHT 사람이 개입하는 자리는 마지막 알림 이후 승인 단계뿐 — 매 회차 점검 결과와 일일 보고가 빠짐없이 저장됨



Source: OPENMARU OpsKnow 정기 점검 1회의 자동 저장 순서

Wallboard와 전국 Dashboard의 Hub & Spoke

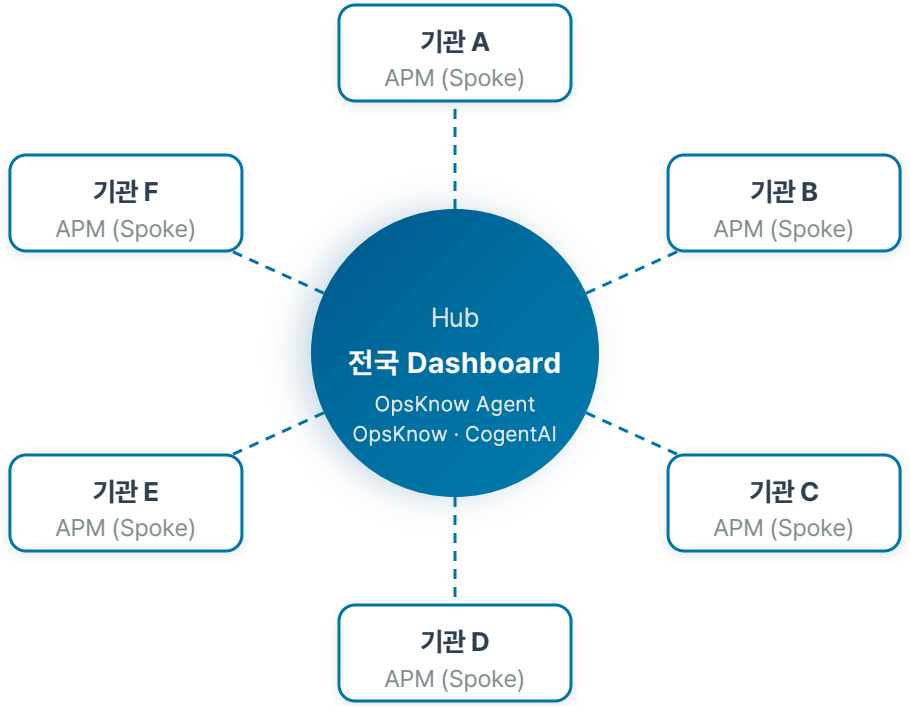
KEY INSIGHT 판정 규칙·임계치·보고 양식을 Hub 한 곳에서 관리함 — 기관 사이에 판정 기준이 달라지지 않음

기관 운영실 Wallboard — 실시간 지표와 당일 판정



왼쪽 예방점검 결과(A1 우선, 미완료 색 구분) · 가운데 지연 트랜잭션과 이상 그룹 · 오른쪽 승인 대기

상급 기관 전국 Dashboard — 등급별 이행 현황



Spoke는 지표 수집과 표준 인터페이스만, Hub가 판정·저장·언어 모델 처리 · A1·A2는 개별 목록, A3·A4는 기관별 집계

Source: OPENMARU Wallboard · OPENMARU Dashboard · 등급 수는 2026-08-27 행정안전부 발표

PART 05

AAS 위 OpsKnow Agent의 통제 구조

판정은 결정적 코드, 결정은 사람, 설명은 AI가 맡는 공공 운영용 설계

역할 분리

1회용 승인 코드

작업 경계와 실행 기록

판정 주체와 설명 주체의 분리

KEY INSIGHT 감사 때 같은 입력으로 다시 실행해 같은 결과를 확인할 수 있음 — 모델 교체 뒤에는 설명 문장만 검증하면 됨

LLM
전달

관리자 문장을 코드에 전달

→

결정적 코드
해석·판정

요청 해석, 점검 명령 선택, 기준 대비 판정

→

사람
승인

운영 책임자가 조치 승인, 승인 코드 입력

→

LLM
설명

판정 결과와 근거를 문장으로 요약

비교 항목	LLM이 판정까지 맡는 방식	결정적 코드가 판정하는 방식
같은 입력의 결과	실행마다 표현과 결론이 달라질 수 있음	**늘 같은 판정값**
감사 때 재현	당시 응답을 다시 만들기 어려움	**같은 입력으로 다시 실행해 같은 결과 확인**
판정 근거	설명 문장 속에 섞여 있음	**판정값과 근거 수치가 따로 남음**
기준 변경 관리	프롬프트 수정에 의존	**판정 규칙의 변경 이력으로 관리**

이원 관리 모델은 운영팀이 필요에 따라 교체하고, 판정 규칙은 결재를 거쳐 변경 — SOP 변경관리 기록에 함께 남김

Source: OPENMARU OpsKnow Agent 설계 · AAS(AI Agent Studio) 위 동작

승인 코드로만 받는 사람의 결정

KEY INSIGHT 적용 직전 상태가 점검 때와 다르면 중단하고 다시 승인받음 — 결재 기록이 그대로 감사 증적이 됨

점검 판정과 근거 → **코드 발급** 30분 · 1회용 → **코드 입력** 운영 책임자 → **직전 재확인** 점검 때와 비교 → **적용** 조치 실행 → **재점검** 같은 규칙 재판정

관리자 입력별 에이전트 동작

✓ 유효한 승인 코드	적용 직전 재확인 뒤 적용
✗ "네" 같은 동의 표현만	적용하지 않음 (승인 코드 필요)
✗ 유효 시간이 지난 코드	적용하지 않음
✗ 이미 사용한 코드	적용하지 않음

적용 직전 재확인

점검 때와 같음
→ 적용 진행

점검 때와 다름
→ 중단, 새 점검·재승인

감사 때 남는 기록

- 판정 상태와 근거 수치
- AAS가 남긴 승인자 계정·승인 시각
- 재확인 결과 (다르면 중단 사유)
- 적용 뒤 재점검 판정

Source: OPENMARU OpsKnow Agent 승인 코드 절차

에이전트 작업 경계와 결재 대상

KEY INSIGHT 권한 상한을 문서 한 장으로 설명할 수 있음 — 위탁 운영 계약 조항과 보안성 검토 답변의 근거가 됨

처음부터 에이전트 범위 밖에 둔 작업

제외 작업	서비스 영향	롤백 위험
재부팅	서비스 중단이 바로 발생	기동 실패 시 복구 판단 필요
설정 변경 실행	미들웨어·DBMS 동작 전체에 영향	복원 방법이 시스템별로 제각각
제품 설치본(zip/tar) 패치	패키지 관리자 밖이라 버전 추적 곤란	원본 보관·복원을 사람이 관리
패키지 삭제·다운그레이드	의존 패키지에 연쇄 영향	이미 적용한 보안 수정이 되돌려질 수 있음

승인 코드로 실행하는 결재 6종

- **임계치 조정**
- **WAS 재시작**
- **인스턴스 증설·감축**
- **세션 강제 종료**
- **외부 시스템 재시작**
- **DB 풀 크기 변경**

절차: 점검 → 승인 코드 → 적용 직전 재확인 → 재점검

위탁 운영 계약 조항 예

판정
판정 규칙 변경은 발주기관 승인

조치
서버 변경은 승인 코드 입력 시에만

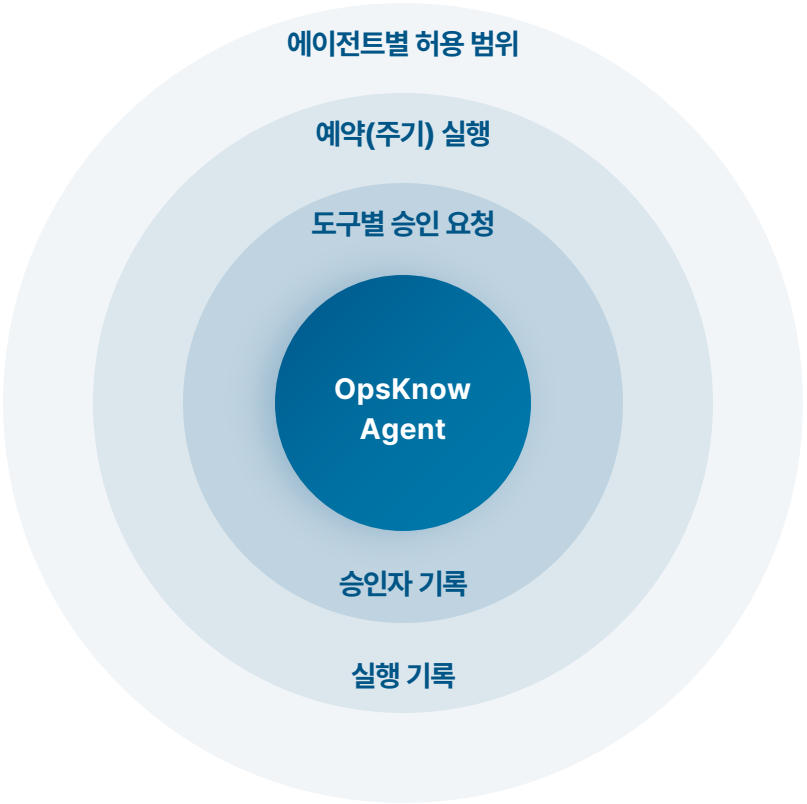
제외 작업
재부팅·설정 변경 실행·설치본 패치·패키지 삭제 미수행

기록
판정·승인·적용·재점검 보관, 정기 보고 포함

Source: OPENMARU OpsKnow Agent 작업 범위 정의

AAS 통제점과 결재 라인 기록

KEY INSIGHT 판정·승인 규칙이 코드와 AAS 설정에 들어 있음 — 인사 이동이나 위탁 사업자 교체가 있어도 같은 절차가 이어짐



예: A1 담당은 점검·보고만, 낮은 등급 담당은 승인 코드 패치까지 허용

결재 라인 기록

단계	주체	남는 결과
요청	관리자	자연어 요청 문장
판정	결정적 코드	대상 서버, 판정 상태, 근거 수치
승인	운영 책임자	1회용 승인 코드 입력, 승인자 계정·시각
적용	OpsKnow Agent	적용 직전 재확인 결과, 적용 결과
확인	결정적 코드	재점검 판정 상태
설명	30B 내부 sLLM	결과 요약 문장

Source: AAS(AI Agent Studio) 에이전트 실행 기반



PART 06

소버린 AI Level 3 폐쇄망 운영

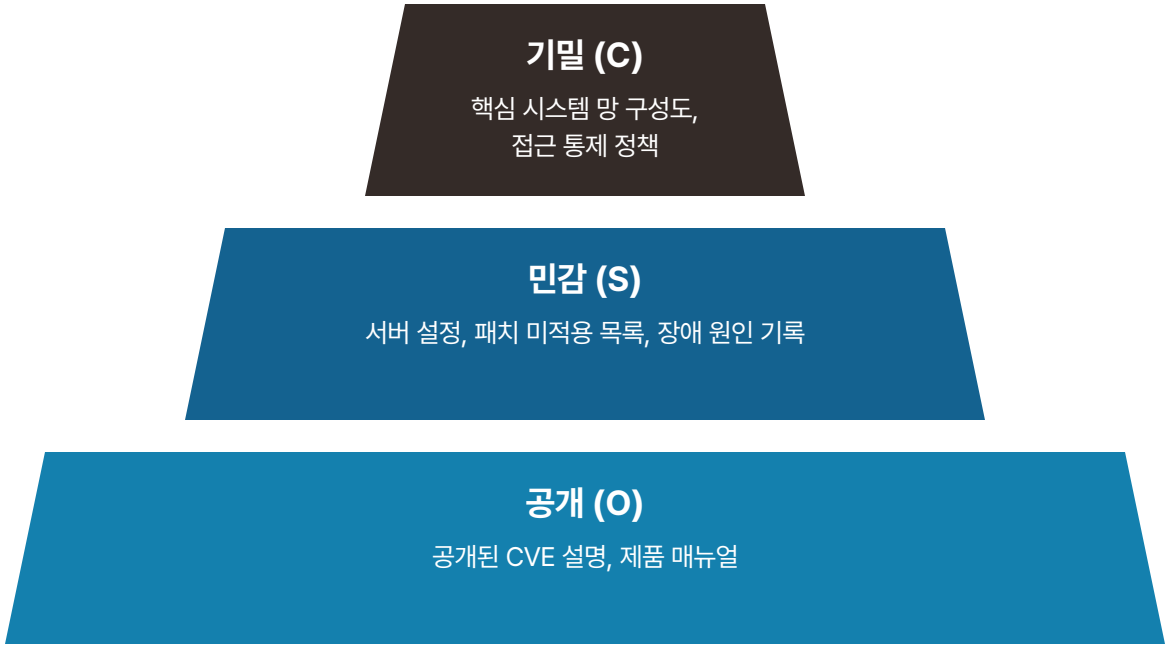
GPU 1대에서 실행하는 30B 수준 내부 sLLM과 외부 송신 0건 판정 기준

- N2SF 등급과 전송 위험
- Level 1~3 판정 기준
- GPU 1대 구성과 비용

운영 데이터의 외부 LLM 전송 위험

KEY INSIGHT 공개 CVE에 미조치 서버 정보가 결합되면 공격 대상 목록이 됨 — 예방점검 데이터는 처음부터 내부 모델로 처리하는 편이 맞음

N2SF 3등급과 예방점검 데이터 (판단 예시)



→ 내부 처리

→ 내부 모델 처리 권장

→ 기관 조건을 갖추면 전송 검토

약 280개 보안 통제 · 11종 정보 서비스 모델 — 등급별 통제를 갖추면 허용하는 조건부 체계

외부 LLM API 사용 시 위험

정보 노출
설정·취약점·장애 기록이 제공사 서버를 거쳐 감

서비스 중단
제공사 장애·회선 단절 때 점검 보고 정지

정책 변경
약관·보관 기간·단가를 제공사가 결정

내부 sLLM은 세 위험을 기관 망 안에서 통제

Source: 국가정보원 N2SF 가이드라인 1.0(2025-09-30), 바이라인네트워크·보안뉴스(2025) · 등급별 판단은 예시

소버린 AI 단계별 판정 기준

KEY INSIGHT 측정 가능한 시험으로 판정함 — 검수 조건과 운영 중 주기 점검을 같은 시험으로 걸 수 있음

Level 1 — BUILT-IN

필수 기준
제품 안 AI 기능

판정 방법
기능 시연과 기능 목록

Level 2 — ON-PREM

필수 기준
LLM·임베딩·벡터DB·가드레일을 기관 서버에 설치

판정 방법
설치 구성 확인

Level 3 — AIR-GAPPED

필수 기준
인터넷 차단 상태에서 동작,
외부 LLM API 호출 0건, GPU 1대

판정 방법
외부 송신 전면 차단 시험, 연결 로그 0건

Level 3 외부 송신 차단 시험

1 차단 정책 적용
기관 망 밖으로 나가는 연결 모두 차단

2 기능 실행
자연어 질의·점검 판정·보고서 작성

3 로그 수집
외부 연결 시도 0건

4 기록 위치 확인
모델 입출력 기록이 기관 서버에만

RFP 문안
검수 시 외부 송신 전면 차단 상태에서 시험해 외부 연결 로그 0건을 입증

소버린 AI 5원칙

나가지 않음	추론 중 외부 송신 0건
사람이 결정	되돌릴 수 없는 동작은 승인 뒤
끌 수 있음	AI를 꺼도 본래 기능 동작
들여다볼 수 있음	모델·프롬프트·입출력 기록 보관
감당할 수 있음	GPU 1대 사양에서 재현

Source: OPENMARU 소버린 AI 단계 정의

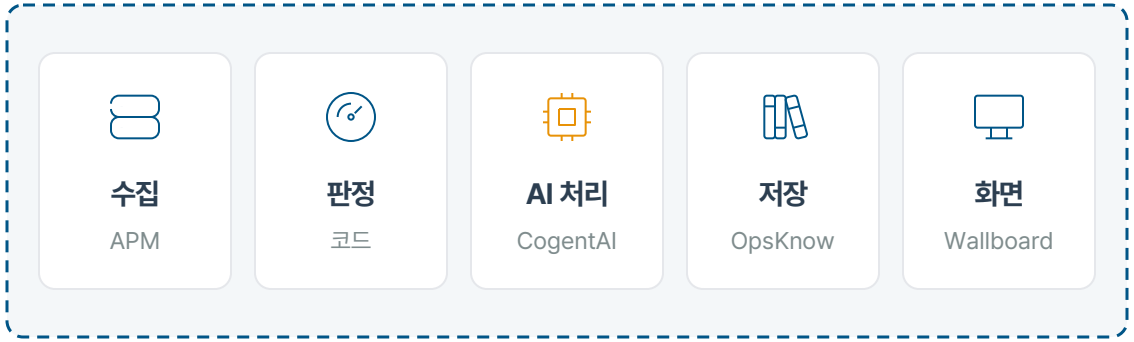
내부 sLLM 구성의 자원과 비용

KEY INSIGHT 예산 산정 단위를 GPU 서버 1대로 고정할 수 있음 — 외부 단가·약관 변경과 서비스 중단 위험에서 분리됨

역할별 필요 자원

역할	맡는 주체	필요 자원
지표 수집	APM 수집기	GPU 불필요
기준 대비 판정	결정적 코드	일반 CPU 서버
요청 해석·결과 설명	30B 내부 sLLM	GPU 장비 1대
조치 승인	사람(승인 코드)	별도 자원 없음

폐쇄망 5계층 — 기관 망 안에서 끝나는 흐름



GPU 서버 1대 단위 비용 항목

GPU 장비	sLLM·임베딩·벡터DB·가드레일 함께 실행	일회성
상면·전력	랙 공간, 전력, 냉각	연간 고정
유지보수	하드웨어 유지보수, AI 엔진 기술지원	연간 고정
오프라인 반입	모델·보안 업데이트 반입 검사	연간 고정

외부 LLM API 대비 위험

위험	외부 API	내부 sLLM
단가 변경	연중 바뀔 수 있음	**도입 뒤 고정비 중심**
약관 변경	기관 동의 없이 바뀔 수 있음	**기관 정책 그대로**
모델 교체	구형 종료 시 강제 교체	**검증 뒤 기관이 결정**

Source: OPENMARU CogentAI 폐쇄망 구성 · 금액은 견적으로 산정

PART 07

보안 취약점 점검의 지능화

KISA·CVE 권고 접수부터 승인 코드 적용과 재점검까지

- 영향 서버 상태 판정
- 승인 코드 기반 패치
- 권고 조치 기간 관리

보안 권고 영향 서버의 상태 판정

KEY INSIGHT 다섯 상태는 조치 필요 여부와 지금 조치 가능 여부에 함께 답함 — "취약/양호" 두 값으로는 미해결 사유가 사라짐

1. **권고 정보 확인** — CVE 번호, 영향 패키지, 수정 버전
2. **설치 목록 수집** — 서버별 OS 패키지 목록 (RPM 등)
3. **저장소 수정본 확인** — 기관 저장소에 수정 버전이 있는지

판정 상태	판정 근거	보고 방식	다음 조치
이미 조치됨	설치 버전이 권고의 수정 버전 이상	조치 완료	없음 (증적만 보관)
설치돼 있지 않음	영향 패키지가 서버에 없음	해당 없음	없음
저장소에 수정본 없음	취약 버전 설치, 저장소에 수정 버전 미등록	미해결	저장소 동기화 확인 후 재대조
보안 정보 없음	저장소가 해당 패키지 권고 정보를 제공하지 않음	판정 불가	담당자 수동 확인
지원 종료 OS	공급사 지원이 끝나 수정본이 나오지 않음	미해결 별도 관리	교체·격리 계획 수립

승인 요청 대상은 따로 모음

"취약 버전 설치 + 저장소에 수정본 있음" 서버만 승인 요청 · 압축 설치본 미들웨어·DBMS는 따로 점검해 같은 목록에 올림

Source: 한국인터넷진흥원 보호나라&KrCERT/CC 보안공지 · KNVD 취약점 정보포털

승인 코드 기반 패치와 조치 현황표

KEY INSIGHT 패치 작업이 곧 증적을 만드는 과정이 됨 — 재점검 결과가 "이미 조치됨"이 아니면 완료로 기록하지 않음

점검 권고 대조 결과 → **승인 요청** 서버·패키지·적용 버전 → **직전 재확인** 하나라도 다르면 정지 → **적용** OS 패키지 패치 → **재점검** "이미 조치됨" 확인

권고별 조치 현황표 — 각 칸은 실행 기록에서 직접 나온 값

열	담는 내용	원천 기록
권고 식별	보호나라 공지 번호, CVE 번호	권고 수신 기록
영향 서버 수	상태별 서버 수와 승인 요청 대상	대조 결과
승인 이력	승인자, 승인 시각, 대상 서버	승인 코드 발급 기록
적용 결과	적용 결과, 바뀐 패키지 버전	적용 실행 기록
재점검 결과	조치 후 상태	재점검 대조 결과
미해결 사유	수정본 없음, 지원 종료 OS, 판정 불가 — 감사에서 가장 자주 쓰임	상태 판정 기록

미들웨어·DBMS 취약점은 점검·보고 뒤 사람이 승인해 조치

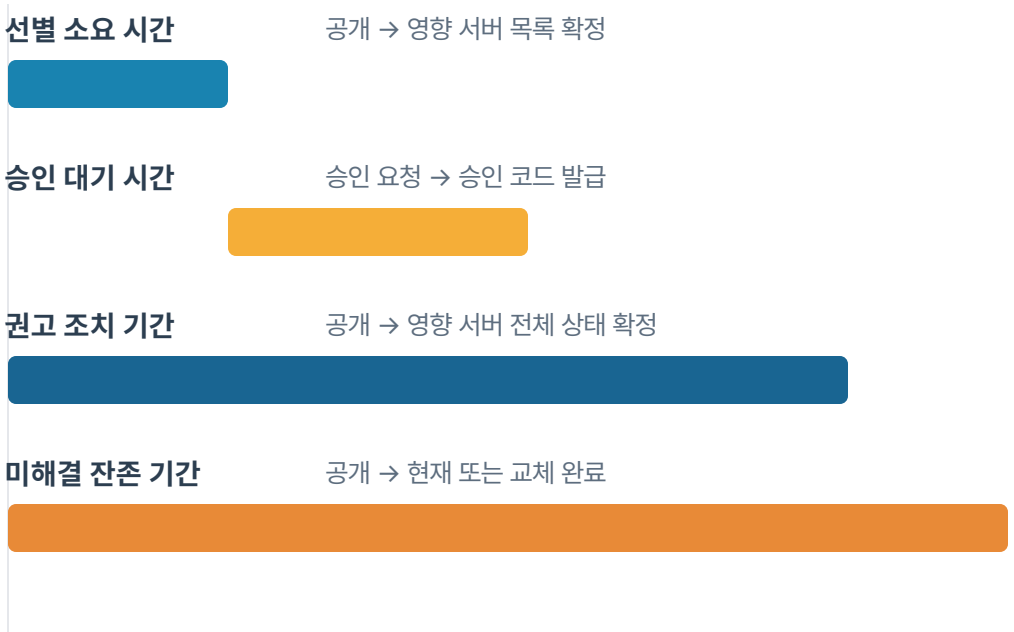
Source: OPENMARU OpsKnow Agent 패치 절차 · 권고별 조치 현황표

권고 조치 기간 관리와 작업 분리

KEY INSIGHT 선별은 빠른데 승인 대기가 길면 승인 절차를, 미해결 잔존이 길면 교체 예산을 먼저 손봄 — 지표가 조치 순서를 정함

권고 조치 기간을 구성하는 시간 지표

시작: 보호나라 공지·CVE 공개 시각으로 고정 · 막대 길이는 개념 예시



분기 일괄 패치는 다음 작업일까지 전체가 공격 가능 기간 → 권고 단위 처리로 전환

작업 분리

작업	OpsKnow Agent	사람
권고 수신·영향 서버 선별	실행	결과 확인
OS 패키지 패치 적용	승인 코드 받아 실행	승인 코드 발급
적용 뒤 재점검·이력 기록	실행	결과 확인
재부팅이 필요한 패치	실행하지 않음	시간대 결정·실행
미들웨어·DBMS 취약점	점검·보고, 조치안	조치 승인
제품 설치본 패치	실행하지 않음	승인 뒤 실행
지원 종료 OS 대응	미해결 목록 관리	교체·격리 결정

Source: OPENMARU 권고 조치 기간 지표 정의 · 시작 시각은 보호나라 게시 시각

PART 08

OpsKnow 운영 기록 통합과 결재 경계

Incident·예방점검 결과·정기 보고를 한 저장소에 쌓고 자동 처리와 결재를 나눔

- 3대 자산의 연결 키
- Incident 기록 항목
- 자동 처리와 결재 경계

OpsKnow 자산 간 연결 키

KEY INSIGHT 연결 키는 저장소 도입 시점에 정해야 함 — 트랜잭션 ID 없이 "오후 2시경 지연"만 남기면 원자료 보관 기간 뒤 증명할 수 없음



점검 이상 → Incident → 정기 보고 인용 → 재발방지 → 임계치 조정

세 자산을 잇는 연결 키

연결 키	예방점검 결과	Incident	정기 보고
시스템 식별자(등급 포함)	점검 대상 지정	장애 시스템 지정	시스템별·등급별 집계
트랜잭션 ID	성능 판정 근거	원인 요청 추적	주요 장애 근거 링크
사이트 태그	센터·위치 구분	발생 위치 구분	사이트별 묶음 보고
운영자 ID	판정 확인자	수행자·승인자	기간별 조치 이력

과업지시서 문안 예

"예방점검 결과, 장애 기록, 정기 보고는 시스템 식별자와 트랜잭션 ID로 상호 조회가 가능해야 함"

Source: OPENMARU OpsKnow 3대 자산 구조 · 행정안전부 표준운영절차(2024-10)

Incident 기록 항목 정의

KEY INSIGHT 담당자가 직접 쓰는 칸은 재발방지뿐 — 나머지는 원인 분석이 끝나면 채워져 감사 3질문에 바로 답함

자동 후보

원인

직접·근본 원인, 확정은 담당자 검토

예: WAS 스레드 풀 포화, 원인은 외부 연계 응답 지연

자동

조치

장애 해소를 위해 실제로 한 일

예: 결재 후 WAS 재시작, 연계 타임아웃 값 확인

담당자 입력

재발방지

바꾼 기준·설정·절차

예: 연계 응답 시간 임계치 추가

자동

관련 트랜잭션 ID

원인을 보여 주는 요청의 추적 ID

예: APM 트랜잭션 추적 ID

자동

사이트 태그

센터·위치·서비스 구분

예: 주 센터 / 재해복구 센터

자동

운영자 ID

조치 수행자와 승인자

예: 수행자·승인자 계정

자동

자동 RCA 시간

원인 후보를 좁히는 데 걸린 시간

예: 분석 시작·종료 시각

감사 3질문

1. 언제 무엇 때문에 났는가
2. 누가 어떤 권한으로 조치했는가
3. 무엇을 바꿨는가

Source: OPENMARU OpsKnow Incident 기록 구조

자동 처리와 결재 대상의 경계

KEY INSIGHT 경계 기준은 되돌릴 수 있는지와 서비스에 영향을 주는지 — 위탁 운영 계약의 운영자 권한 조항에 그대로 옮길 수 있음

자동 처리 3종

기록 누락 방지 — 빠진 날짜는 미점검으로 읽힘

알림 발송

주의·위험 판정 시 담당자에게 즉시

남는 기록: 발송 시각·수신자·판정 항목

OpsKnow 저장

판정 결과·근거 지표·Incident 초안

남는 기록: 시스템 식별자·트랜잭션 ID

임계치 보고서 생성

초과 항목을 시스템·기간별로 묶음

남는 기록: 보고서 원본과 원자료 범위

결재 6종 — 승인 코드 절차를 거침

결재 대상	서비스 영향	결재 때 확인할 지표
임계치 조정	이후 판정 기준이 바뀜	최근 지표 분포, 과거 Incident
WAS 재시작	처리 중 요청 중단, 일시적 지연	스레드·힙 메모리, 트랜잭션 ID
인스턴스 증설·감축	처리 용량과 비용 변화	사용률 추이, 예상 부하
세션 강제 종료	사용자 작업 중단	장기 점유 세션 목록
외부 시스템 재시작	연계 서비스 일시 중단	연계 응답 시간
DB 풀 크기 변경	동시 연결 수·메모리 변화	커넥션 사용률, 대기 시간

Source: OPENMARU OpsKnow Agent 자동 처리·결재 경계 매트릭스

원자료 기반 정기 운영 보고

KEY INSIGHT 같은 범위로 다시 만들면 같은 수치가 나옴 — 감사 답변이 "수치 + 저장 위치 + 기록 시점" 형태가 됨

일간

판정, 주의·위험 항목, 당일 Incident

매일 생성 · 쓰임: 일상점검 수행 증적

주간

반복된 주의 항목, 결재 조치 내역

매주 생성 · 쓰임: 운영 회의 자료

월간

시스템별 장애 건수·조치 시간, 임계치 변경

매월 생성 · 쓰임: SLA 월간 산출 근거

분기

등급별 추이, 재발 장애, 재발방지 이행

분기마다 생성 · 쓰임: 기관 보고·위탁 운영 평가

연간

한 해 장애 추이, 점검 기준 변경, 개선 과제

매년 생성 · 쓰임: 기본계획·연간 시행계획 근거

원자료 재생성 원칙

보고서마다 생성에 쓴 원자료 범위를 기록하고,
상위 주기는 하위 주기를 다시 집계함

수치 **저장 위치** **기록 시점**

감사 답변의 세 요소

연간 보고 → 계획 문서

등급별 장애 추이	→ 기본계획 중점 대상
재발방지 이행	→ 시행계획 개선 과제
기준 변경 이력	→ 차년도 점검 기준
결재 조치 내역	→ SLA 목표·평가 기준

Source: OPENMARU OpsKnow 정기 운영 보고 · 수치는 코드 계산, 문장은 30B 내부 sLLM 작성

PART 09

관리자 사용 장면과 응답 예시

자연어 요청 한 줄에서 점검 보고서와 조치 승인까지 네 가지 업무 장면

월간 점검 결과

분기 감사 준비

보안공지·장애 직후

월간 점검 결과 자연어 요청

KEY INSIGHT 항목마다 대상·판정·근거·조치 제안이 함께 나옴 — 자료가 없는 항목은 정상에 합산하지 않고 따로 표시함

"이번 달 OS와 미들웨어, DBMS 점검 결과 보여 줘"

1. **요청 접수** LLM
   문장을 그대로 코드에 전달
2. **의도 해석** 코드
   영역·기간 추출, 조회 명령 선택
3. **조회** 코드
   OS 지표와 APM 미들웨어·DBMS 지표
4. **판정** 코드
   기준값 비교, 정상·주의·이상
5. **설명** LLM
   판정 결과로 요약, 증적 첨부

OpsKnow Agent 응답

이번 달 예방점검 결과 요약

OS ○대	미들웨어 ○개	DBMS ○개
정상 ○ · 주의 ○ · 이상 ○	정상 ○ · 주의 ○	정상 ○ · 이상 ○

이상 **업무서버 A 데이터 디스크 사용률 기준값 초과**
조치 제안: 로그 보관 정책 점검 (담당자 작업)

이상 **DBMS B 장시간 잠금 반복 · 근거: APM 잠금 대기 기록**
조치 제안: 해당 트랜잭션 확인 (조회만, 결재 불필요)

주의 **WAS C 커넥션 풀 사용률이 기준값에 근접**
조치 제안: DB 풀 크기 변경 검토 (결재 필요)

첨부: 영역별 판정표 · 항목별 원값과 수집 시각 · 적용 기준 목록

자료 없는 항목은 "수집 자료 없음"으로 별도 줄에 표시

Source: OpsKnow Agent 응답 예시 · 서버 이름·IP는 가리고 개수는 ○로 표기

분기 감사 준비와 보고서 초안

KEY INSIGHT 미이행을 찾으려면 판정이 필요함 — 담당자 시간이 자료 수집에서 초안 검토로 옮겨 감

"이번 분기 미이행 점검 항목 알려 줘"

미이행 판정 기준

① 점검 주기 안에 결과 기록이 빈 항목

② 이상 판정 뒤 조치 기록이 이어지지 않은 항목

응답: 일상점검 결과 없음 ○건 · 조치 미완료 ○건 / 특별점검 결과 없음 ○건
근거 목록: 점검 주기, 마지막 결과·시각, 이상 근거, 조치 기록 유무

근거 대조 3요소

수치	저장 위치	기록 시점
초안의 숫자	OpsKnow 원 기록	만들어진 때

Wallboard 분기 현황: 영역별 이행률 · 조치 미완료 건수 · 승인 대기 목록 (보고서와 같은 판정 결과)

분기 운영 보고서 초안 검토 단계

1. **초안 생성** — OpsKnow Agent
   분기 점검 결과·Incident·월간 보고 집계
2. **근거 대조** — IT 담당자
   초안 수치와 OpsKnow 원 기록 일치 확인
3. **해석 문장 수정** — IT 담당자
   원인 서술과 개선 계획 문장
4. **확정** — 관리자
   미이행 항목의 후속 계획
5. **보관** — 자동
   확정본을 증적으로 저장 (HWP·출처 링크)

Source: OpsKnow Agent 응답 예시 · 개수는 ○로 표기

보안공지 발표일의 영향 서버 조치

KEY INSIGHT "네"나 "진행해"로는 적용되지 않음 — 적용 전후 버전과 승인 기록이 함께 회신되어 그대로 증적이 됨

"오늘 나온 보안공지 영향 서버 찾아 줘"

응답: 대상 서버 상태별 분류

조치 필요 O대 취약 버전 설치, 수정본 있음	→ 승인 코드 입력 후 적용
이미 조치됨 O대 수정 버전 이상 설치	→ 증적으로 기록
설치돼 있지 않음 O대 대상 패키지 없음	→ 증적으로 기록
저장소에 수정본 없음 O대 기관 저장소에 수정본 없음	→ 저장소 갱신 요청
보안 정보 없음 O대 판정에 필요한 정보 없음	→ 담당자 확인
지원 종료 OS O대 공급사 지원 종료	→ 전환·보완 대책 결정

승인 코드 입력에서 재점검 회신까지

1. **조치 제안**
   "조치 필요" 서버 O대에 수정 버전 적용 제안
2. **승인 코드 입력**
   발급 후 30분 · 한 번만 사용, "네"로는 적용 안 함
3. **적용 직전 재확인**
   점검 때와 다르면 멈추고 보고
4. **적용**
   OS 패키지 패치
5. **재점검 회신**
   적용 전후 버전과 판정을 회신

Source: OpsKnow Agent 응답 예시 · KISA 보호나라&KrCERT/CC 보안공지 기준 · 개수는 O로 표기

장애 직후 유사 Incident 검색

KEY INSIGHT 응답은 "원인 후보"까지만 냄 — 원인 확정은 담당자가 하고 그 결과가 새 Incident로 쌓임

"방금 장애와 비슷한 과거 사례 찾아 줘"

응답: 유사 Incident O건

1 WAS C 응답 지연 — 원인 후보

원인: DB 커넥션 풀 고갈

조치: 풀 크기 조정 (결재 후) · 재발방지: 풀 사용률 임계치 보고서 추가

2 WAS C 응답 지연

원인: 배치 작업과 업무 시간대 겹침

조치: 배치 시각 변경 · 재발방지: 배치 일정 점검 항목 추가

원인 후보 1번 · 근거: APM 커넥션 풀 사용률 추이

제안 조치: DB 풀 크기 변경 — 결재 필요

자동 처리: 담당자 알림 발송, Incident 케이스 저장

장애 직후 응답에서의 처리 구분

조치	구분	응답에서의 처리
담당자 알림 발송	자동	즉시 처리, 결과 표시
Incident 케이스 저장	자동	즉시 처리, 저장 결과 표시
임계치 보고서 생성	자동	생성 후 첨부
임계치 조정	결재	조정안과 근거만 제시하고 멈춤
WAS 재시작	결재	영향 범위와 근거만 제시
인스턴스 증설·감축	결재	필요 규모 근거만 제시
세션 강제 종료	결재	대상 세션 목록만 제시
외부 시스템 재시작	결재	영향 범위와 근거만 제시
DB 풀 크기 변경	결재	변경안과 근거만 제시

Source: OpsKnow Agent 응답 예시 · 개수는 O로 표기

PART 10

경쟁 방식 비교와 차년도 사업 준비

판정·증적 범위 비교, 도입 효과 측정 지표, 요구사항 선택 순서

- 판정·증적 범위 비교
- 효과 측정 지표
- 요구사항과 RFP 문안

경쟁 방식과의 판정·증적 범위 비교

KEY INSIGHT A사·B사 자료는 일상점검 양식 보고에서 멈춤 — 제안 평가표에는 수집 항목보다 판정 근거와 조치 기록 범위를 먼저 둠

비교 기준	A사 방식	B사 방식	OPENMARU 방식
AI 판정·설명	언급 없음	언급 없음	**결정적 코드 판정 + 내부 sLLM 설명**
특별점검·구조진단	범위 밖	결과 기록 지원 · 구조진단 외부 위탁	**같은 저장소에 결과 보관**
장애·변경 관리	ITSM 연동에 맡김	ITSM 연동에 맡김	**Incident·승인 기록을 점검 이력과 연결**
보안 취약점 조치	범위 밖	범위 밖	**대상 선별 → 승인 → 적용 → 재점검**
이력 보관 기간	보관 기간 제한	자료에 명시 없음	**기관이 정한 감사 대상 기간 이상**
배포 형태	설치형 전용	자료 기준 확인 필요	**기관 보안 정책에 맞춘 구성**
폐쇄망 AI	없음	없음	**소버린 AI Level 3 (외부 송신 0건)**

공통점: 두 회사 모두 "임계치 설정만으로는 감사 대응이 어렵다"는 문제의식은 같으나 해결 기능은 범위 밖

Source: A사·B사 2026년 하반기 배포 공공 예방점검 자료(익명) · OPENMARU 분석

도입 전후 효과 측정 지표

KEY INSIGHT 시작·종료 시각을 기록 원천으로 고정해야 비교가 성립함 — 확인한 날부터 재면 늦게 볼수록 기간이 짧게 나오는 왜곡이 생김

점검 소요 시간

속도

시작
점검 시작

종료
마지막 항목 판정 기록

권고 조치 기간

속도

시작
보호나라 게시일

종료
재점검 결과 기록

원인 규명 시간

속도

시작
장애 인지

종료
원인 필드 기록

보고서 작성 시간

속도

시작
보고 주기 마감

종료
결재 상신

증적 누락 건수

품질

산식
누락 건수 / 전체 점검·조치 건수

누락 판정
판정 근거·승인·재점검 누락

기준선 측정 절차

1. 범위 확정 → 2. 기록 수집 → 3. 시각 추출 → 4. 값 산출 → 5. 기준선 확정

조건: 착수 전 분기 보고 주기 1회 이상, 보안공지 대응·장애 처리 1건 이상 포함 · 등급별 구분 · 목표값은 "기준선 대비 개선"

Source: OPENMARU 도입 효과 측정 기준 · 효과 수치는 기준선 측정 뒤 협의

단계별 요구사항 묶음과 RFP 문안

KEY INSIGHT "AI 판정 기능"처럼 쓰면 사업자마다 다르게 해석함 — 검수할 수 있는 문장으로 적어야 감사 때 다시 보여 줄 수 있음

자가진단 단계 → 요구사항 묶음

체계 없음	지표 수집·판정 기록·이력 저장	APM · OpsKnow
단순 자동화	판정 근거·승인 코드 조치·재점검·이력 연결	OpsKnow Agent · AAS
지능화	폐쇄망 AI·보안 권고 대응·보고 재생성·장기 보관	CogentAI · Wallboard · Dashboard

시연 요청 때 준비할 항목

- 대상 시스템 등급과 수
- 점검 영역(OS·미들웨어·DBMS)
- 점검 주기
- 망 구성(폐쇄망 여부)
- 보안공지 처리 방식
- 현재 보고 양식

RFP 기능 요구사항 문안 5개

1. **판정 근거 기록**
   항목별 판정과 판정에 쓴 수치·비교 기준을 함께 기록하고, 같은 원자료로 재판정하면 같은 결과
2. **조치 승인 기록**
   서버를 바꾸는 조치는 1회용 승인 코드 입력 시에만 실행, 적용 직전 상태가 다르면 정지
3. **폐쇄망 AI**
   AI 판정 설명·보고서 작성이 외부 LLM 호출 없이 기관 GPU 장비에서 동작함을 시험으로 입증
4. **보고서 재생성**
   일·주·월·분기·연 보고서를 원자료에서 다시 만들어 원본과 대조 가능
5. **이력 보관 기간**
   예방점검·장애·조치 이력을 감사 대상 기간 이상 보관, 같은 화면에서 조회

Source: OPENMARU 차년도 요구사항 문안 예시 · 등급은 확정 통보 기준

THANK YOU

예방점검 지능화 도입 상담과 OpsKnow Agent 시연 요청

대상 시스템 등급·점검 영역·점검 주기 기준으로 기관 환경에 맞춘 시연 준비

OPENMARU

OpsKnow · OpsKnow Agent · APM · CogentAI

https://www.openmaru.io/

02-6953-5427

hello@opennaru.com

© OPENMARU. All rights reserved.