

# AI 기반 OS 자동화 점검 서비스 도입 제안서

수동 점검의 한계를 넘어 AI와 자동화로 실현하는  
스마트 서버 관리 플랫폼 JARVIS

Client

고객사명

Date

2026. 04.

By

CywellSystem



24/7 자동 점검



이상 자동 감지



보고서 자동화



AI 기반 분석

## TABLE OF CONTENTS

# 제안서 구성

문제 정의부터 기대효과와 도입 로드맵까지 핵심 내용을 한 번에 확인합니다.

01 수동 점검의 한계와 문제점

06 자산·관리 기능 소개

02 AI 자동화의 필요성

07 운영·보안 기능 소개

03 JARVIS 시스템 개요

08 도입 전·후 비교 (AS-IS vs TO-BE)

04 모니터링 기능 소개

09 기대효과 및 비즈니스 가치

05 점검·운영 기능 소개

10 도입 로드맵



80%

점검 공수 절감



24/7

AI 자동 점검 체계



100%

보고서 자동화

제안서 전체는 "자동화 운영 체계 전환"이라는 하나의 스토리로 구성되어 있습니다.



# EXECUTIVE SUMMARY | 핵심 요약

수동 점검에서 자동화 점검으로 전환했을 때의 가장 큰 변화와 가치

JARVIS가 해결하는 것



## 지금의 문제

수동 점검이 야기하는 리스크

- ✘ 수작업 점검으로 인한 누락·오류 상시 발생
- ✘ 이상 발생 후 수 시간 뒤 인지하는 사후 대응 구조
- ✘ 보고서 수작업 작성으로 월 수십 시간 공수 낭비



## JARVIS 솔루션

AI 기반 지능형 플랫폼

- ✔ 경량 Agent 기반 24/7 자동화 점검 체계 구축
- ✔ 임계치 초과 및 이상 패턴 즉시 알림·대응
- ✔ 결과 요약 및 PDF/Word 보고서 자동 생성·배포



## 도입 기대효과

비즈니스 가치 창출

- ✔ 운영 인력 고부가가치 업무 재배치 및 품질 표준화
- ✔ 수시간 단위의 장애 감지를 수분 이내로 획기적 단축 (MTTR 감소)
- ✔ 투명한 이력 관리로 고객 신뢰 및 감사 대응 수준 향상



**핵심 포인트:** 사람이 하던 단순 반복 점검은 JARVIS 시스템이 24시간 대신 수행하고, 운영자는 AI가 분석한 예외 상황 대응과 서비스 품질 개선에 집중합니다.



## PROBLEM ANALYSIS | 수동 점검의 한계

기존 수동 운영 방식이 갖는 6가지 구조적 문제를 운영 현실 관점에서 정리

왜 바뀌어야 하는가?

### 시간·비용 낭비

- 서버당 30분 이상 수작업 소요
- 월 수십 시간의 비효율적 공수 발생

### 점검 누락 위험

- 휴일 및 야간 시간대 점검 사각지대
- 체크리스트 누락에 의한 장애 방치

### 사후 대응 한계

- 이상 발생 후 수 시간 뒤 인지 구조
- 선제적 예방 불가 및 서비스 타격

### 보고서 부담

- 수많은 데이터의 수작업 취합 및 작성
- 휴먼 에러 발생 및 문서 형식 불일치

### 담당자 의존성

- 퇴직 및 부서 이동 시 노하우 소실
- 경험에 의존한 불완전한 인수인계

### 감사 대응 불가

- 과거 점검 이력 보관 및 추적 미흡
- 보안 컴플라이언스 및 정기 감사 취약

#### ① 현재 상태 | 수동 점검 중심 운영

문제의 본질은 점검 자체보다 "지속 가능하지 않은 운영 구조"에 있습니다. 이제는 단순한 모니터링을 넘어, 자동화된 분석과 **AI 기반 설명 가능성**을 통해 운영의 일관성을 확보해야 합니다.



# WHY AI NOW? | 왜 지금 AI 자동화 점검인가

탐지 중심 모니터링을 넘어, 운영자의 의사결정을 지원하는 진정한 AI 보조가 필요합니다.



AI 자동화 점검



## 기존 자동화의 한계

- × 이벤트 알림은 많지만, 무엇이 진짜 중요한지 사람이 다시 해석해야 함
- × 복합 이슈(CPU+Memory+Network) 발생 시 상관관계 분석 어려움
- × 원인 설명과 조치 가이드가 없어 단순 관제 알림 수준에 머무름



## JARVIS AI가 만드는 변화

- ✓ 여러 점검 결과를 종합하여 분석 후 위험 우선순위 자동 식별 및 제시
- ✓ 단순 임계치 초과 알림을 넘어 현상의 "근본 원인 후보"를 문장으로 설명
- ✓ 운영자가 즉시 참조하고 실행할 수 있도록 권장 조치 제안

VS

## 고객사 관점의 가치



### 운영 품질 일관성

담당자 개개인의 숙련도 편차를 줄여 상향 평준화된 운영 품질 확보



### 제안 경쟁력 강화

단순 관제가 아닌 "AI 운영 고도화" 메시지로 타사 대비 제안 차별화



### 효율 및 신뢰 향상

장애 사전 예방, 리소스 운영 효율화, 투명한 감사 대응 체계 마련

## AI 기반 4단계 운영 최적화 프로세스

탐지 Detect

01

Agent 기반 실시간 데이터 수집 및 임계치/패턴 이상 유무 확인

분석 Analyze

02

단일 이벤트가 아닌 여러 지표 간의 상관관계 및 연쇄 패턴 해석

설명 Explain

03

기술적 로그를 번역하여 파급 영향과 원인 후보를 문장으로 제시

실행 Act

04

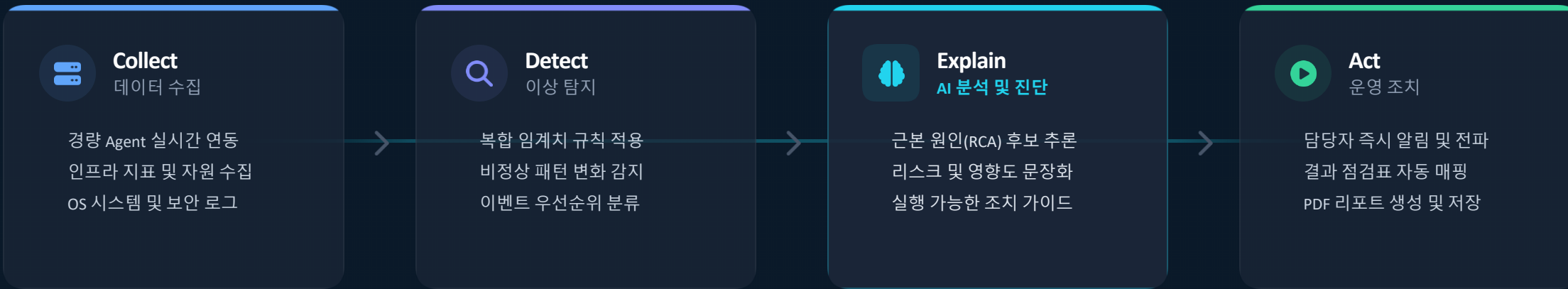
운영자가 즉각 검토하고 조치할 수 있는 권장 Action 가이드 제공



# SYSTEM OVERVIEW | JARVIS 시스템 개요

에이전트 기반 실시간 수집부터 AI 분석, 자동 보고까지 통합 관제 프로세스를 제공합니다.

● 엔터프라이즈 아키텍처



## Supported Environments

- Linux
- Windows
- Unix

## Architecture Flow

대상 서버 (Agent) → 수집/전송 (TLS) → 중앙 관제 플랫폼 (AI/Rule) → 점검 운영 및 보고

## 실시간 모니터링

대시보드를 통한 인프라 자원 및 파티션  
사용량 통합 가시성 확보

## AI 이상 진단

이벤트 패턴 분석을 통한 장애 원인 식별  
및 권장 조치 가이드 제공

## 통합 자산 관리

고객사, 그룹, 호스트 단위의 체계적인  
자산 정보 및 라이프사이클 관리

## 점검 보고서 자동화

수집된 데이터와 AI 분석 결과를 바탕으로  
원클릭 정기 점검 문서 생성



# MONITORING FEATURES | 실시간 가시성

복잡한 인프라 자원 상태와 AI 분석 결과를 한 화면에서 직관적으로 파악합니다.



실시간 가시성

## 인프라 기본 정보

서버 식별을 위한 필수 자산 정보 및 운영 가동 시간을 제공합니다.

## 실시간 자원 활용도

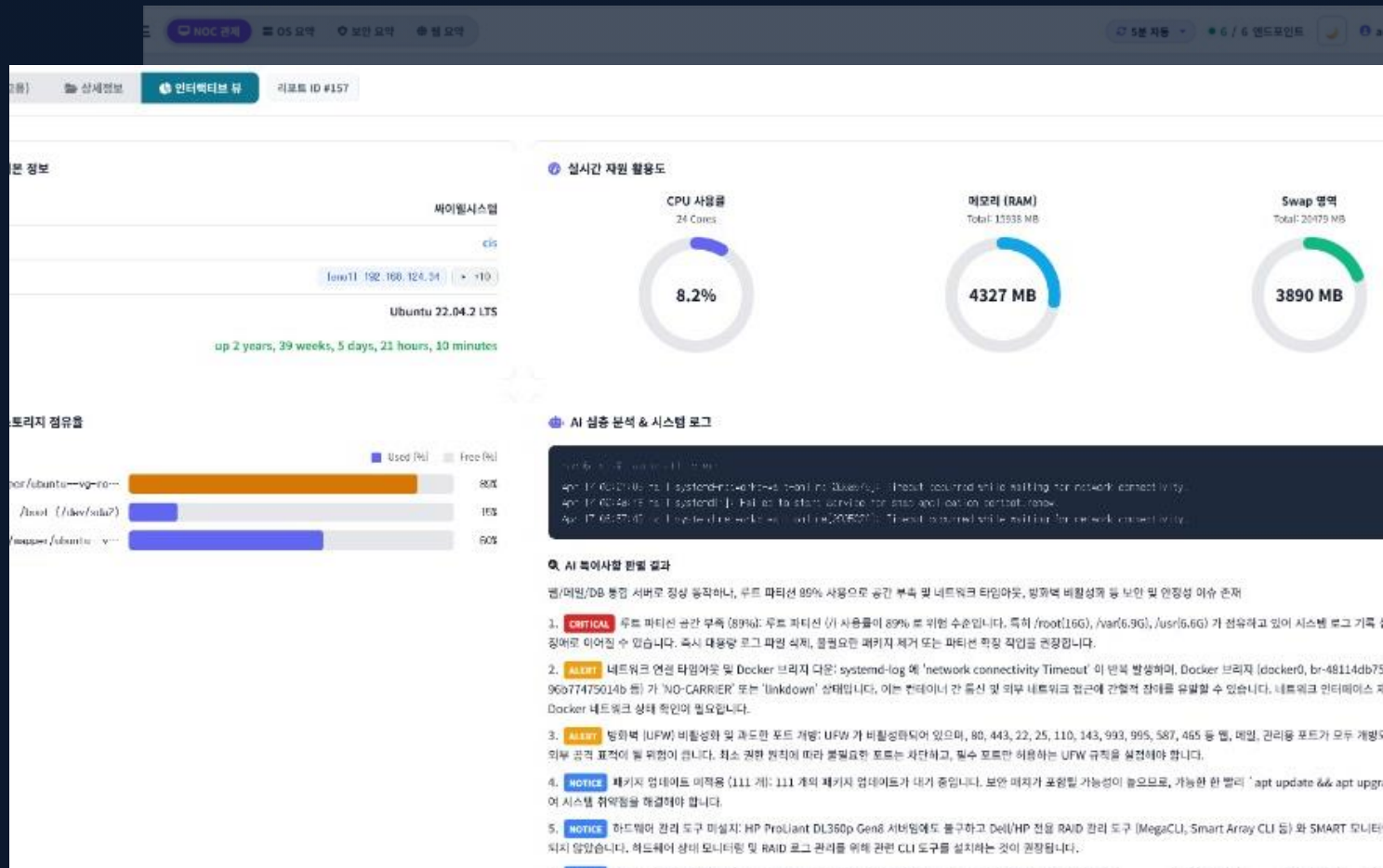
CPU, Memory, Swap 리소스 현황을 직관적인 도넛 차트로 모니터링합니다.

## 파티션 스토리지 점유율

마운트 지점별 디스크 사용량 및 위험 임계치를 시각적 막대로 제공합니다.

## 시스템 로그 & AI 진단

시스템 주요 로그 문맥과 AI의 이상 판별 결과를 결합하여 판단 근거를 제시합니다.



운영 효과

⚡ 상태 즉시 확인

🛡️ 위험 요소 선제 식별

🧠 운영 의사결정 일관성



# AI DIAGNOSIS | 설명 가능한 분석

단순 알림을 넘어, 이벤트의 근본 원인과 파급 영향을 자연어로 설명하고 권장 조치를 제시합니다.

AI 로그 분석

## 원인 후보 추론

장애 발생 시 연관 로그와 메트릭을 종합 분석하여 핵심 이슈의 **근본 원인(Root Cause)**을 식별합니다.

## 리스크 문장화

단순 수치 경고를 넘어 서비스 중단, 성능 저하 등 비즈니스에 미치는 **파급 영향을 자연어로 설명**합니다.

## 권장 조치 제시

담당자가 즉각적으로 수행할 수 있는 프로세스 재시작, 파티션 정리 등의 **구체적 Action 가이드**를 제공합니다.

MITTR 단축

허위 경보 감소

설명 책임 강화

AI 진단센터

[Homepage] 메모리 위험 — 2026-04-22 09:08

Homepage 2026-04-22 00:08:40

AI 진단센터

0  
Critical 이벤트

이벤트 90%

이벤트 목록

AI 신뢰도

발생

진단

발생

발생

진단완료

발생

발생

진단완료

시스템 상태

호스트: WAS (172.24.23.11) | memory: 92.9% (임계치: 90.0%)

이슈 사항

**AI분석**  
**단순 메모리 사용률에 대한**  
**알림 메시지가 아닌 원인 추론.**  
**또한 조치 권장 사항을 스스로**  
**제시**

계치 초과. ps 분석 결과, PID 228847 의 'homepage-0.0.1-SNAPSHOT.jar' 애플리케이션이 전체 메모리 사용량의 25.8% 를 점유하여 주요 원인을 확인함. 해당 프로세스는 Java 기반이며, 장시간 (489 시간) 실행 중이므로 메모리 누수 (Memory Leak) 또는 과도한 캐시/오브젝트 축적이 의심됨.

AI 분석 요약

메모리 사용률이 92.9% 로 임계치 초과. ps 분석 결과, PID 228847 의 'homepage-0.0.1-SNAPSHOT.jar' 애플리케이션이 전체 메모리의 약 25.8% 를 점유하여 주요 원인을 확인함. 해당 프로세스는 Java 기반이며, 장시간 (489 시간) 실행 중이므로 메모리 누수 (Memory Leak) 또는 과도한 캐시/오브젝트 축적이 의심됨.

권장 조치 명령

```
echo 'Memory usage is critical due to PID 228847. Please investigate heap dump or restart the application service if necessary.'
```

추가 권장 사항

- PID 228847 프로세스의 Java Heap Dump 를 생성하여 메모리 누수 지점을 분석하세요.
- 임시 조치로 해당 서비스 (homepage) 를 재시작하여 메모리 사용량을 초기화할 수 있습니다.
- 장기적인 해결을 위해 애플리케이션의 GC 로그를 확인하고 메모리 설정 (Xmx) 을 재검토하세요.

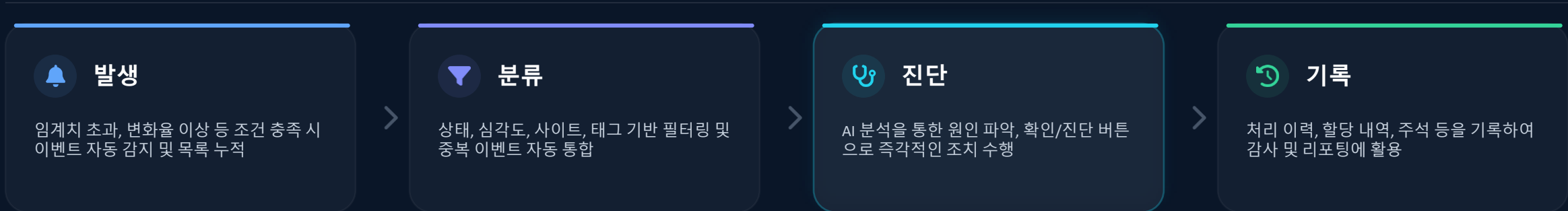


# INSPECTION & OPERATION | 점검·운영 기능

Event Center를 통한 발생, 분류, 진단, 기록의 일관된 운영 흐름을 제공합니다.

▶ 이벤트 중심 운영

## Event Center 운영 흐름



발생

임계치 초과, 변화율 이상 등 조건 충족 시 이벤트 자동 감지 및 목록 누적

분류

상태, 심각도, 사이트, 태그 기반 필터링 및 중복 이벤트 자동 통합

진단

AI 분석을 통한 원인 파악, 확인/진단 버튼으로 즉각적인 조치 수행

기록

처리 이력, 할당 내역, 주석 등을 기록하여 감사 및 리포팅에 활용

## 주요 작업 액션 및 운영 지표

### 이벤트 처리 액션

- 확인** 단순 인지 및 처리 완료 표기
- 진단** AI 상세 분석 및 원인 파악 요청
- 할당** 특정 운영 담당자에게 티켓 이관
- 무시** 유지보수 등 예외 상황 처리
- 주석** 조치 내역 및 향후 참고 사항 메모

Critical 이벤트

**0**

Warning 이벤트

**8,793**

진단 진행중

**2**

AI 보고서

**30**



# REPORTING FEATURES | 자동 보고서 생성

정형 데이터와 AI 요약이 결합된 보고서를 One Click으로 자동 생성합니다.

⚡ 100% 보고서 자동화

## 정형 점검표 + AI 요약

자산/자원/디스크 상태를 정형 표로 구성  
이상 항목에 대한 AI 서술형 원인 요약  
고객 친화적인 문서 가독성 확보

## 1-Click 공유 및 내보내기

PDF, Excel 문서 즉시 다운로드  
이메일 연동을 통한 링크 공유  
프로세스 간소화

## 템플릿 및 이력 관리

고객사별 맞춤형 점검 양식 제공  
과거 점검 결과 버전 관리 및 추적  
정기 감사 및 컴플라이언스 대응 완벽

점검 항목	점검 내용	비고
Base Infra	Uptime	up 6 years, 34 weeks, 1 day, 18 hours, 35 minutes
	cpu	Model : Intel(R) Xeon(R) Bronze 3104 CPU @ 1.70GHz
		수량 : 6 Core %user : 1.0 / %system : 2.0 / %iowait : 0 / %idle : 97.0
	Memory	Physical Memory : 7216 (MB)
		User : 6146 (MB) / Free : 363 (MB) Buffer/Cache 미포함
	swap	Total Swap : 16379 (MB)
Used : 6730 (MB) / Free : 9649 (MB)		
System Log	에러 로그 확인됨	
Hardware LED		
Network	Interface em1 172.24.23.11	

PDF 다운로드

### AI 점검 종합 의견

**[정상]** 전체 자원 사용률이 안정적이며, 주요 프로세스가 정상 가동 중입니다.  
**[주의]** 단, /dev/sda2 파티션 사용률이 77%로 지속 증가 추세이므로, 1개월 내 용량 확보 및 로그 파일 정리를 권장합니다.

✔ 점검 문서 양식 표준화

↓ 문서 작성 시간 50% 절감

↳ 대외 전달 문서 품질 향상



# ASSET & MANAGEMENT | 통합 관리 기능

복잡한 인프라를 체계적으로 관리하고, 철저한 권한 및 이력 추적을 제공합니다.

통합 관리 기능

## 체계적인 4단계 계층 구조 관리



**고객사 (Client)**

최상위 논리적 단위



**사이트 (Site)**

물리적/논리적 위치



**그룹 (Group)**

서비스/용도별 분류



**호스트 (Host)**

개별 대상 서버

## 사용자 및 권한 관리

역할 기반 접근 제어 (RBAC)

최소 권한 원칙 적용

다중 인증(MFA) 및 세션 관리

## 유연한 검색 및 태깅

사용자 정의 태그 부여

다중 조건 필터링 검색

대규모 인프라 빠른 식별

## 감사 및 이력 중앙화

시스템 작업 이력 로깅

Agent 상태 및 배포 이력

컴플라이언스 증적 자료 활용



# OPERATION & SECURITY | 운영·보안 기능

엔터프라이즈 수준의 강력한 보안 설계와 무중단 운영을 위한 견고한 아키텍처를 제공합니다.

● 엔터프라이즈 표준



## TLS / 프록시 보안

Agent와 중앙 서버 간의 모든 통신 구간을 완벽히 암호화하며, 망분리 환경을 위한 안전한 프록시 아키텍처를 지원합니다.



## 최소 권한 원칙 (RBAC)

강력한 역할 기반 접근 통제를 통해 관리자 및 시스템 프로세스에 필요한 최소한의 권한만 부여하여 침해 위협을 원천 차단합니다.



## 오프라인 버퍼링

일시적인 네트워크 단절이나 서버 점검 시에도 Agent 단에서 점검 데이터를 자체 보관하고 연결 시 자동 복구하여 유실을 방지합니다.



## 수평 확장 아키텍처

수천 대 이상의 대규모 엔터프라이즈 환경에서도 시스템 병목 현상 없이 유연하게 성능을 분산 및 확장 (Scale-out)할 수 있습니다.



## 백업 및 재해복구(DR)

시스템 장애나 예기치 않은 데이터 센터 재난 상황에 대비하여 정기적인 데이터 백업 및 신속한 서비스 복구 체계를 갖춥니다.



## 투명한 감사 로깅

점검 정책 변경, 중요 알림 설정, 관리자 로그인 등 시스템 내에서 발생하는 모든 핵심 행위를 빠짐없이 기록하여 완전한 추적성을 보장합니다.



## 정책 기반 임계치 및 규칙 운영

단일 기준이 아닌 고객사, 사이트, 서버 그룹별로 상이한 비즈니스 중요도에 맞춰 세밀한 점검 정책과 알림 임계치를 유연하게 적용하고 중앙에서 통제합니다.



# AS-IS vs TO-BE | 전환 효과 비교

수동 점검의 한계를 넘어 AI 자동화 점검으로의 혁신적 전환을 제시합니다.

## AS-IS (현재)

수동 점검 중심 운영

## TO-BE (도입 후)

AI 자동화 점검 체계

탐지 리드타임

### 수 시간 ~ 수 일 소요

담당자 순회 점검에 의존, 정기점검 일시 및 야간/휴일 사각지대 발생



### 수 분 이내 즉시 탐지

Agent 기반 24/7 무중단 모니터링 체계 가동

점검 공수

### 서버당 최소 30분 수작업

서버 수 증가 시 인력 추가 투입 불가피, 비효율 심화



### 단순 반복 공수 80% 절감

사람은 고부가가치 분석 및 예외 대응 업무에 집중

보고 품질

### 담당자별 편차 발생

수작업 취함으로 인한 휴먼 에러, 서식 불일치 문제



### 100% 균일한 표준 양식 제공

정형 데이터 기반의 무결점 자동 생성 보고서 산출

설명 가능성

### 개인 경험 의존형 해석

현상만 나열, 고객사 보고 시 근본 원인 설명 부족



### AI 조치 가이드

이상 발생 원인, 영향 범위, 명확한 해결 방안 문장 제시

컴플라이언스

### 이력 관리 및 증적 미흡

과거 이력 추적 곤란, 외부 보안 감사 대응 시 취약



### 완전한 시스템 감사 로깅

모든 점검 데이터와 사용자 조치 이력 영구 보존

✔ 사람이 하던 반복 점검을 시스템이 대신 수행하고, 사람은 예외 대응과 **운영 품질 고도화**에 집중하는 구조로 전환됩니다.



# EXPECTED BENEFITS | 기대효과 및 비즈니스 가치

AI 자동화 점검 도입을 통해 얻을 수 있는 정량적/정성적 비즈니스 가치입니다.

ROI 극대화

## 장애 복구 시간 (MTTR)



### 30~60% ↓

AI 원인 분석을 통해 즉각적인 조치가 가능해져 **서비스 정상화 시간 획기적 단축**

## 무의미한 허위 경보



### 30~50% ↓

상관관계 및 패턴 분석 기반 필터링으로 **운영자 알림 피로도 최소화**

## 정기 점검·보고 공수



### 50% ↓

데이터 취합 및 리포트 작성 완전 자동화로 **비핵심 반복 업무 제거**

## 서비스 가용성 및 안정성 향상



24/7 무중단 감시 체계와 사전 이상 징후 탐지를 통해 비계획적 다운타임을 원천 차단하고 서비스 품질(SLA)을 높입니다.

## 완벽한 규제 준수 및 감사 대응



모든 점검 내역과 운영자 조치 이력을 시스템에 투명하게 기록하여 강화되는 정보보호 보안 감사에 대응합니다.

## 재무적 가치 Financial Value

인력 운영 효율화를 통한 **전체 IT 운영 비용(TCO) 절감**  
장애 발생 시 **기회비용 손실(SLA 위반 페널티 등) 방지**  
시스템 노후화 예측으로 **최적의 인프라 투자 타이밍 확보**

## 비재무적 가치 Non-financial Value

반복 업무 제거로 **IT 부서의 고부가가치 업무 집중도 향상**  
설명 가능한 AI 가이드로 **운영자 숙련도 편차 극복 및 피로도 감소**  
안정적인 서비스 환경 구축을 통한 **대내외 비즈니스 신뢰도 상승**



# ROI ANALYSIS | 정량 효과

수동 점검 공수 절감에 따른 재무적 가치와 투자 회수 기간을 분석합니다.

정량적 효과 분석

## 운영 환경 가정치 (AS-IS)

관리 대상 서버 100 대

서버당 월 점검 시간 (정기/수시 포함) 1 시간

월간 총 점검 시간 100 시간

엔지니어 시간당 인건비 80,000 원

현재 연간 수동 점검 비용

**96,000,000 원**

(월 400만원 × 12개월)



JARVIS 자동화 도입



**- 85%**

점검 소요 시간 단축

(월 100시간 → 15시간)



연간 1,020 시간 확보

핵심 부가가치 업무로 인력 재배치



## 기대 재무 효과 (TO-BE)

연간 총 절감액 (Annual Savings)

**81,600,000 원**

기존 수동 점검 비용 대비 85% 절감

투자 회수 기간 (Payback Period)

**3.5 개월**

도입 1년 차에 손익분기점(BEP) 조기 달성

3년 누적 투자 수익률 (ROI)

**315 %**

솔루션 도입 TCO 대비 압도적인 투자 수익성 보장

※ 상기 산출 내역은 일반적인 엔터프라이즈 환경을 가정한 시뮬레이션 결과이며, 실제 라이선스 비용 및 고객사별 절감액은 사전 기술 검증(PoC) 진행 후 최종 확정됩니다.



# IMPLEMENTATION ROADMAP | 도입 로드맵

성공적인 서비스 전환을 위한 4단계 표준 방법론을 제시합니다.



STEP 01

## 준비 및 설계

### ☑ 주요 활동

요구사항 수집 및 분석  
보안 정책 및 망 연동 협의  
점검 대상 및 범위 확정

### 📄 산출물

WBS (작업 분할 구조도)  
시스템 아키텍처 설계서

RACI:

공동 책임



STEP 02

## 구축 및 연동

### ☑ 주요 활동

수집 Agent 배포 및 설치  
중앙 관제 플랫폼 구축  
초기 임계치 및 점검 규칙 설정

### 📄 산출물

설치 결과 보고서  
초기 설정 명세서

RACI:

수행사(R) / 고객사(A)



STEP 03

## 안정화 및 교육

### ☑ 주요 활동

오탐지/과탐지 튜닝 (Tuning)  
시범 운영(PoC) 리포트 검토  
운영자 및 사용자 교육

### 📄 산출물

사용자 매뉴얼  
시범 운영 결과 보고서

RACI:

수행사(R) / 고객사(A)



STEP 04

## 운영 전환 및 확장

### ☑ 주요 활동

정식 서비스 오픈 (Go-Live)  
전사 대상 사이트/서버 확대  
AI 자동화 를 고도화

### 📄 산출물

최종 검수 및 완료 보고서  
월간 정기 점검 리포트

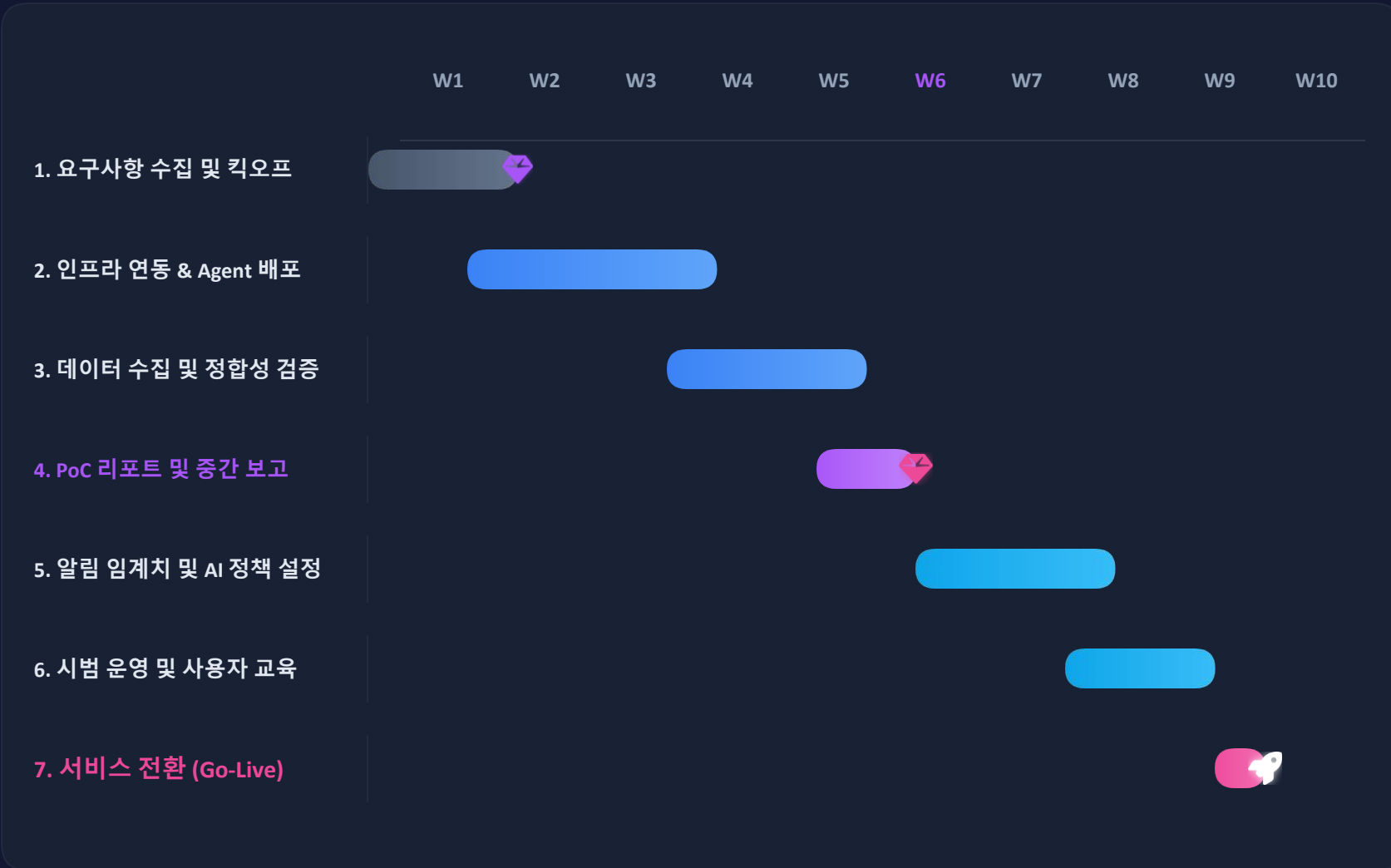
RACI:

고객사(R) / 수행사(S)



# SCHEDULE & MILESTONES | 예상 일정 및 마일스톤

체계적인 프로젝트 관리와 명확한 게이트 검수를 통해 성공적인 도입을 보장합니다.



## 게이트 / 검수 포인트

Gate 1 (W2)

### 설계 및 환경 검증

- 대상 서버 리스트 확정
- 네트워크/방화벽 오픈 확인

Gate 2 (W5-W6)

### PoC 완료 검수

- 데이터 수집 정합성 99% 이상
- 자동화 보고서 샘플 승인

Gate 3 (W10)

### 최종 오픈 승인

- 운영자 교육 수료
- 기존 수동 점검 이관 확정



# SUMMARY & NEXT STEPS | 제안 요약 및 향후 계획

JARVIS 도입을 위한 핵심 가치와 구체적인 다음 단계를 제안합니다.

## 가시성 (Visibility)

실시간 대시보드를 통해 인프라 현황부터 상세 리소스까지 투명하게 파악하여 장애 대응 골든 타임을 확보합니다.

## 설명력 (Explainability)

단순 수치가 아닌 AI의 문장형 원인 분석과 조치 가이드를 통해 누구든 직관적으로 이해하고 대응할 수 있습니다.

## 활용성 (Usability)

이벤트 처리부터 정형 보고서 자동 생성까지, 일련의 운영 과정을 통합하여 담당자의 업무 피로도를 획기적으로 줄입니다.


## Next Steps


- 1 PoC 범위 합의**  
대상 시스템 및 필수 검증 시나리오 확정
- 2 보안 검토 및 계정 발급**  
사전 보안 요건 확인 및 테스트 인프라 접근 권한 부여
- 3 프로젝트 킥오프**  
상세 일정 조율 및 프로젝트 공식 착수

## Contact Us

성공적인 운영 자동화 전환을 위해 전담 컨설턴트가 상세히 안내해 드립니다.

 (주) 싸이웰시스템 영업본부

 crcho@cywell.co.kr

 010-5396-0872