

Resume - Jaecheol Lee

Jaecheol Lee

2025-12-24

Contents

1	이재철	2
1.1	연락처	2
1.2	학력	2
1.3	경력 요약	2
1.3.1	보유 기술	2
1.3.2	자격증 및 교육	2
1.3.3	금융 보안 전문성	3
1.4	경력 경로 분석	3
1.4.1	Phase 1: 인프라 기반 구축 (2017-2019)	3
1.4.2	Phase 2: 자동화 및 DevOps 전환 (2019-2022)	3
1.4.3	Phase 3: 금융 보안 및 AI 통합 (2022-현재)	3
1.4.4	향후 방향	4
1.5	경력사항	4
1.5.1	아이티센 CTS 정보보안 운영 엔지니어	4
1.5.2	가온누리정보시스템 프리랜서 인프라 엔지니어	5
1.5.3	관텍투자일임 인프라·정보보호팀 인프라 엔지니어	6
1.5.4	편엔씨 DevOps 엔지니어	7
1.5.5	조인트리 인프라·시스템 엔지니어	7
1.5.6	메타넷애플랫폼 인프라·시스템 엔지니어	7
1.5.7	엠티데이터 서버·시스템 엔지니어	8
1.6	주요 프로젝트	8
1.6.1	실전 보안 운영 자동화 플랫폼 (2024 ~ 현재)	8
1.6.2	Nextrade 대체거래소 인프라 구축 및 운영	9
1.6.3	대규모 콜센터 원격근무 전환	10
1.6.4	금융 클라우드 보안 아키텍처	11
1.6.5	AI 기반 인프라 자동화 플랫폼 (2024.09 ~ 현재)	11
1.7	기술 스택	15
1.7.1	보안 솔루션	15
1.7.2	클라우드 및 가상화	15
1.7.3	자동화 및 개발	15
1.7.4	AI/ML 및 자동화	16
1.7.5	컨테이너 및 오케스트레이션	16
1.7.6	네트워크	16
1.8	자격증	16

1 이재철

인프라·보안 엔지니어

1.1 연락처

- 전화: 010-5757-9592
 - 이메일: qws941@kakao.com
 - 주소: 경기도 시흥시 장현천로61, 307동 1301호
 - GitHub: github.com/qws941
-

1.2 학력

- 한양사이버대학교 컴퓨터공학과 (2024.03 ~ 재학중)
 - 용남고등학교 졸업 (2013)
-

1.3 경력 요약

총 경력: 8년 8개월 (2017.02 ~ 현재)

1.3.1 보유 기술

- 보안: FortiGate 방화벽, DDoS, IPS, WAF, NAC, DLP, EDR, APT, Splunk SIEM
- 클라우드: AWS (EC2, VPC, IAM, S3), Docker, Kubernetes, Cloudflare Workers
- 자동화: Python, Shell, Ansible, Terraform, n8n
- 모니터링: Grafana, Prometheus, Loki, Sentry
- DevOps: GitLab EE, CI/CD, Container Registry, Docker Compose
- AI/ML: Claude AI, ML 기반 위협 예측 및 자동 라우팅 시스템, MCP 서버 통합
- 금융 규제: 금융감독원 감사 대응, ISMS-P, ISO27001, FSC 본인가

1.3.2 자격증 및 교육

- 진행 중: CISSP 준비
- 계획: CISM 취득 예정
- AWS Certified Solutions Architect 준비 중
- 한양사이버대학교 컴퓨터공학과 재학 (2024.03 ~)

1.3.3 금융 보안 전문성

- 금융감독원 감사: 분기별 감사 대응 및 보안 요구사항 이행
 - FSC 본인가: 금융위원회 본인가 사전 심사 대응 완료
 - 망분리 설계: 다계층 망분리 및 Air-Gap 구축
 - 재해복구: DR 운영 및 분기별 테스트
 - 규제 준수: ISMS-P, ISO27001 이행
 - 운영 규모: 대규모 거래 시스템 운영
-

1.4 경력 경로 분석

8년 이상의 경력을 통해 인프라 운영 → 보안 자동화 → 금융 보안 전문가로 성장해왔습니다.

1.4.1 Phase 1: 인프라 기반 구축 (2017-2019)

핵심 역량: 서버·네트워크 운영, 방화벽 관리, 망분리 구축

- 한국항공우주산업(KAI) 상주 운영으로 대규모 인프라 운영 경험 축적
- Linux 서버, 방화벽, IDS 정책 관리 및 로그 분석 역량 확보
- 제조망-개발망 물리적 분리 구축으로 보안 아키텍처 이해도 향상
- 성과: 방화벽 처리 성능 200% 향상, 보안 사고 0건 달성

1.4.2 Phase 2: 자동화 및 DevOps 전환 (2019-2022)

핵심 역량: Python/Ansible 자동화, 클라우드 아키텍처, CI/CD 보안

- 메타넷오피스플랫폼에서 대규모 재택근무 환경 구축 및 VPN/NAC 통합
- Python 기반 네트워크 자동화 도구 개발로 운영 효율성 극대화
- Ansible 정책 자동 배포 시스템 구축
- AWS 클라우드 아키텍처 설계 및 Kubernetes 마이그레이션 경험
- 성과: 작업 시간 95% 절감, NAC 정책 배포 90% 단축

1.4.3 Phase 3: 금융 보안 및 AI 통합 (2022-현재)

핵심 역량: 금융 규제 준수, AI 기반 위협 분석, 보안 자동화 플랫폼

- 금융투자업 보안 인프라 설계·구축·운영 전 과정 경험
- FSC 본인가 보안 분야 완벽 대응 (지적사항 0건)
- Claude AI 기반 위협 정보 자동화 시스템 구축
- n8n 워크플로우 기반 보안 운영 자동화 플랫폼 개발
- Splunk-FortiNet 통합 관제 시스템으로 SIEM 역량 강화

- 성과: MTTR 87% 개선, 수동 분석 90% 자동화, 감사 지적사항 0건

1.4.4 향후 방향

- CISSP/CISM 자격 취득: 글로벌 보안 전문가 인증
 - 클라우드 보안 심화: AWS Security Specialty, CCSP 준비
 - AI/ML 보안 연구: 위협 예측 모델 고도화, 자동 대응 시스템 확장
-

1.5 경력사항

1.5.1 (주)아이티센 CTS | 정보보안 운영 엔지니어

2025.03 ~ 현재 (10개월) | Nextrade 대체거래소 운영SM (정보보안팀)

프로젝트 규모

- 운영 인프라: 대규모 서버·네트워크 장비
- 일일 거래량: 대량 주문 및 데이터 처리

주요 업무

- SOC 운영: 3교대 보안관제 체계 운영
- 보안 솔루션 관제: 다종 솔루션 통합 관제
- 인시던트 대응: 등급별 SLA 기반 대응
- 재해복구 운영: DR 사이트 관리 및 분기별 테스트
- 취약점 관리: 주간/월간 스캔 및 SLA 기반 패치
- 규제 준수: FSC 분기별 감사, ISMS-P, ISO27001 이행
- 협업: 개발팀·거래팀·운영팀 간 보안 요구사항 조율
- 인시던트 분석: 긴급 보안 사고 시 TF 구성 및 근본 원인 분석

주요 성과 (STAR 방식)

- **Splunk-FortiNet 통합 관제 시스템 구축**
 - Situation: 다수 보안 솔루션의 분산된 로그로 인한 통합 관제 어려움
 - Task: 중앙집중식 보안 관제 시스템 구축 필요
 - Action: Splunk SIEM과 FortiNet 보안 장비 통합, 실시간 대시보드 구축
 - Result: 보안 이벤트 탐지 시간 80% 단축 (평균 30분 → 6분), 정책 배포 시간 75% 감소
- **인시던트 대응 체계 최적화**
 - Situation: 보안 인시던트 발생 시 대응 시간 지연 문제
 - Task: MTTR(평균 복구 시간) 단축을 위한 프로세스 개선
 - Action: 자동화된 인시던트 대응 플레이북 개발, Grafana 실시간 알림 시스템 구축
 - Result: MTTR 87% 개선 (15분 → 2분), 월간 보안 오탐률 95% 감소

- **Claude AI 기반 위협 정보 자동화**
 - Situation: 일일 평균 10,000건 이상의 보안 이벤트 수동 분석 필요
 - Task: 위협 정보 분석 자동화를 통한 업무 효율성 향상
 - Action: Claude AI API 연동, ML 기반 위협 패턴 학습 시스템 구축
 - Result: 수동 분석 작업 90% 자동화, 위협 탐지 정확도 85% 향상, 분석 처리 속도 10배 개선
- **n8n 워크플로우 기반 보안 자동화**
 - Situation: 반복적인 보안 정책 적용 및 취약점 패치 작업
 - Task: API 기반 자동화를 통한 운영 효율성 개선
 - Action: n8n 워크플로우 플랫폼 구축, 20개 이상의 자동화 워크플로우 개발
 - Result: API 처리 성능 300% 개선, 월간 작업 시간 160시간 절감, 인적 오류 제로화
- **금융 규제 준수 100% 달성**
 - Situation: FSC 분기별 감사 및 엄격한 금융 보안 규제 대응
 - Task: 금융감독원 감사 지적사항 최소화
 - Action: 보안 컴플라이언스 자동 점검 시스템 구축, 실시간 규제 준수 모니터링
 - Result: 3분기 연속 감사 지적사항 0건, 취약점 처리 SLA 100% 준수, DR 복구 시간 70% 단축

1.5.2 (주)가온누리정보시스템 | 프리랜서 인프라 엔지니어

2024.03 ~ 2025.02 (11개월) | Nextrade 대체거래소(다자간매매체결회사) 구축 프로젝트

프로젝트 규모

- 신규 구축 인프라: 네트워크/서버/end-point 보안 솔루션 구축/운영
- 금융시스템: 거래 플랫폼, 백오피스
- 사용자: 전사 임직원

주요 업무

- **보안 아키텍처 설계:** 다계층 망분리 및 Air-Gap 구축
- **보안 솔루션 구축:** 시스템보안, 네트워크보안, 엔드포인트보안
- **자동화 개발:** Python 기반 방화벽/NAC/DLP 정책 자동화 시스템
- **FSC 본인가:** 금융위원회 본인가 사전 심사 대응 및 보안 체크리스트 이행
- **DR 인프라 구축:** DR 사이트 설계 및 구축
- **컴플라이언스:** ISMS-P, ISO 27001 인증 준비 및 Gap Analysis

주요 성과 (STAR 방식)

- **Python 기반 보안 정책 자동화 프레임워크 개발**
 - Situation: 1,000개 이상의 방화벽 정책 수동 관리로 인한 오류 발생
 - Task: 정책 관리 자동화 시스템 개발 필요
 - Action: Python 기반 자동화 프레임워크 개발, FortiManager API 통합

- Result: 정책 배포 시간 95% 단축 (2시간 → 6분), 설정 오류율 0% 달성
 - **엔드포인트 보안 최적화**
 - Situation: EPP/DLP 솔루션으로 인한 단말 성능 저하 문제
 - Task: 보안 수준 유지하면서 성능 개선
 - Action: 정책 최적화, 예외 처리 규칙 정교화, 리소스 사용률 모니터링
 - Result: 단말 CPU 사용률 40% 감소, 사용자 생산성 향상, 보안 수준 유지
 - **FSC 본인가 보안 분야 완벽 대응**
 - Situation: 금융위원회 본인가 사전 심사 대비
 - Task: 보안 체크리스트 100% 이행
 - Action: 200개 이상의 보안 요구사항 분석 및 구현, 증적 자료 준비
 - Result: 보안 분야 지적사항 0건, 예정보다 2개월 조기 완료
 - **NAC 자동화로 운영 효율성 극대화**
 - Situation: 신규 단말 접속 시 수동 승인으로 인한 지연
 - Task: 보안성 유지하면서 자동화 구현
 - Action: 조건 기반 자동 승인 시스템 개발, 위험 기반 접근 제어
 - Result: 정책 배포 시간 90% 단축, 월간 처리 건수 500% 증가
-

1.5.3 (주)관텍투자일임 | 인프라·정보보호팀 인프라 엔지니어

2022.08 ~ 2024.03 (1년 7개월) | AI 기반 주식투자 서비스

주요 업무

- 금융보안데이터센터 운영
- 대규모 서버 및 스토리지 형상관리
- 망분리 환경 내 DLP, DB 접근제어, VPN 정책 관리
- AWS 클라우드 보안 구성

주요 성과 (STAR 방식)

- **Python 자동화로 시스템 안정성 향상**
 - Situation: 월 평균 15건의 시스템 장애 발생
 - Task: 장애 예방 및 신속한 복구 체계 구축
 - Action: Python 기반 예방 정비 스크립트 개발, 자동 복구 시스템 구축
 - Result: 월간 시스템 장애 80% 감소 (15건 → 3건), MTTR 60% 단축
- **DB 접근제어 성능 최적화**
 - Situation: DB 접근제어 시스템으로 인한 쿼리 지연
 - Task: 보안 정책 유지하면서 성능 개선
 - Action: 쿼리 패턴 분석, 캐싱 전략 수립, 인덱스 최적화
 - Result: 쿼리 응답 시간 70% 개선, CPU 사용률 50% 감소

1.5.4 (쥬편엔씨 | DevOps 엔지니어

2022.05 ~ 2022.07 (3개월) | 클라우드 인프라

주요 업무

- AWS 클라우드 아키텍처 구축
- Kubernetes 마이그레이션 사전 검토
- Python/Shell 기반 백업·복구 자동화

주요 성과

- 백업/복구 자동화: MTTR 85% 단축 (60분 → 9분)
 - CI/CD 보안 통합: 배포 파이프라인에 보안 스캔 단계 추가, 취약점 사전 차단
 - 컨테이너 보안: 이미지 스캔 자동화, 보안 정책 수립
-

1.5.5 (쥬조인트리 | 인프라·시스템 엔지니어

2021.09 ~ 2022.04 (8개월) | 국민대학교 차세대 정보시스템

주요 업무

- UTM, VMware NSX-T 기반 네트워크 세분화
- NAC, DLP, APT 등 보안 솔루션 통합 운영
- OSS 기반 보안 모니터링 구축

주요 성과

- 네트워크 세분화: 월간 장애 75% 감소 (12건 → 3건)
 - 보안 통합 관제: APT·NAC·DLP 연동으로 침해 시도 100% 차단
 - DLP 정책 최적화: 오탐률 90% 감소, 정탐률 95% 달성
 - 고가용성 구축: 이중화 구성으로 99.9% 가용성 달성
-

1.5.6 (쥬메타넷애플랫폼 | 인프라·시스템 엔지니어

2019.12 ~ 2021.08 (1년 9개월) | 대규모 콜센터 인프라

주요 업무

- 대규모 재택근무 환경 구축
- SSL VPN, NAC 솔루션 통합

- Ansible 기반 정책 자동 배포
- Python 기반 네트워크 스위치 자동 점검 시스템 개발

주요 성과

- **네트워크 자동화**: Python으로 200대 스위치 점검 자동화, 작업 시간 95% 절감
 - **VPN 안정성 개선**: 백신-VPN 충돌 해결로 접속 성공률 99% 달성
 - **Ansible 자동화**: NAC 정책 배포 시간 90% 단축 (3시간 → 18분)
 - **신규 사이트 구축**: 5개 사이트 네트워크 설계 및 무장애 구축
-

1.5.7 (주)엠티데이터 | 서버·시스템 엔지니어

2017.02 ~ 2018.10 (1년 9개월) | 한국항공우주산업(KAI)

주요 업무

- Linux 서버 운영 및 보안 패치
- 방화벽, IDS 정책 관리 및 로그 분석
- DB 접근제어 솔루션 초기 구성

주요 성과

- **방화벽 최적화**: 정책 분석 및 최적화로 처리 성능 200% 향상
 - **망분리 구축**: 제조망-개발망 완전 분리, 보안 사고 0건
 - **취약점 관리**: 월간 점검 체계 구축, 패치 적용률 98% 달성
-

1.6 주요 프로젝트

1.6.1 ☑ 실전 보안 운영 자동화 플랫폼 (2024 ~ 현재)

개인 프로젝트 | Production-Ready Security Operations Platform

GitHub: github.com/qws941

1.6.1.1 보안 통합 관리 플랫폼

- **목적**: 방화벽 실시간 중앙관리 플랫폼
- **기술스택**: Node.js, Cloudflare Workers, JavaScript, REST API, Webhook
- **아키텍처**: 도메인 기반 아키텍처 설계, 방화벽 중앙관리 API 연동
- **핵심기능**:
 - 중앙 집중식 로그 분석 및 정책 검증
 - 방화벽 실시간 데이터 수집 및 정책 위반 자동 탐지

- 대용량 이벤트 처리 시스템
- **운영성과:**
 - 10개 방화벽 중앙 관리, 정책 동기화 시간 95% 단축
 - 정책 검증 자동화로 설정 오류 100% 사전 차단
 - 실시간 위협 분석으로 보안 사고 대응 시간 80% 개선

1.6.1.2 SafeWork Industrial Health Platform

- **목적:** 산업보건 설문조사 SaaS 플랫폼
- **기술스택:** Flask 3.0, PostgreSQL 15, Redis 7, Cloudflare Workers
- **아키텍처:** Cloudflare Workers Edge API 기반 전국 동시 접속 처리, Flask 3.0 하이브리드 아키텍처
- **핵심기능:**
 - 종이 설문 디지털 전환 및 집계 자동화
 - 실시간 데이터 분석 및 리포팅
 - Edge API를 통한 고성능 및 저지연 서비스 제공
- **운영성과:**
 - 종이 설문 대비 집계 시간 99% 단축 (3일 → 30분)
 - 전국 50개 사업장 동시 접속 처리 (지연시간 50ms 이하)
 - 중소기업 30개사 운영 중, 월 활성 사용자 5,000명

1.6.1.3 Public Grafana Dashboard (퍼블릭 대시보드)

- **목적:** 실시간 인프라 모니터링 및 관찰성 플랫폼 공개
- **기술스택:** Grafana, Prometheus, Loki, Tempo, Synology NAS
- **접근:** <https://grafana.jclee.me>
- **핵심기능:**
 - 프로덕션 서비스 실시간 모니터링
 - 메트릭, 로그, 트레이스 통합 대시보드
 - 고가용성 달성 및 실시간 알림 시스템
 - 장기 데이터 보관 및 히스토리 분석
- **운영성과:**
 - 99.5% 가동률 유지 (월간 다운타임 3.6시간 이하)
 - 15개 서비스 통합 모니터링, 실시간 메트릭 제공
 - 알림 응답 시간 평균 2분, 자동 복구율 85%
 - 6개월간 데이터 보관, 트렌드 분석 가능

1.6.2 Nextrade 대체거래소 인프라 구축 및 운영

가온누리정보시스템 + 아이티센 CTS | 2024.03 ~ 현재

프로젝트 개요

- **프로젝트 성격:** 대한민국 신규 대체거래소 구축
- **인프라 규모:** 대규모 서버·단말·네트워크 장비, 대량 주문 처리
- **사용자:** 전사 임직원
- **핵심 시스템:** 거래 플랫폼, 백오피스

구축 단계 (2024.03 ~ 2025.02)

- **역할:** 보안 인프라 설계 및 구축 총괄
- **핵심 아키텍처:**
 - Zero Trust 보안 모델 기반 다계층 망분리
 - 15종 보안 솔루션 통합 (방화벽, IPS, WAF, NAC, DLP, EDR, APT 등)
 - Python 기반 보안 자동화 프레임워크 (5,000줄 이상)
- **주요 성과:**
 - 금융위원회 본인가 사전 심사 보안 분야 지적사항 0건
 - 방화벽 정책 자동화로 배포 시간 95% 단축, 오류율 0%
 - EPP/DLP 최적화로 단말 CPU 사용률 40% 개선
 - 구축 기간 동안 보안 침해사고 0건

운영 단계 (2025.03 ~ 현재)

- **역할:** 정보보안팀 운영 엔지니어
- **핵심 업무:**
 - SOC 24/7 운영 총괄 (3교대 체제)
 - 15종 보안 솔루션 통합 관제 및 인시던트 대응
 - 재해복구 계획 수립 및 분기별 모의훈련
 - 금융규제 준수 (ISMS-P, ISO27001, FSC 요구사항)
- **주요 성과:**
 - 10개월간 보안 침해사고 0건 유지
 - 금융감독원 3분기 연속 감사 지적사항 0건
 - 거래 플랫폼 99.95% 가용성 달성
 - 보안 오탐률 95% 감소, 정탐률 98% 달성
 - DR 복구 시간 70% 단축 (RTO 4시간 → 1.2시간)

기술적 하이라이트:

- **자동화:** Python 프레임워크로 월 160시간 작업 시간 절감
- **컴플라이언스:** ISMS-P, ISO 27001, FSC 요구사항 100% 준수
- **가용성:** 거래 플랫폼 99.95% 가용성, DR RTO 1.2시간 달성
- **보안 성과:** 10개월 무사고 운영, 취약점 SLA 100% 준수

1.6.3 대규모 콜센터 원격근무 전환

메타넷오피스 | 2020

역할: 보안 인프라 구축 리드 규모: 3,000명 동시 접속 기술: SSL VPN, NAC, Ansible, Python 성과: COVID-19 대응 2주 내 구축 완료, 운영 인력 70% 축소

1.6.4 금융 클라우드 보안 아키텍처

관텍투자일임 | 2023

역할: AWS 보안 설계 및 구현 기술: AWS (VPC, IAM, GuardDuty), Python, Terraform 성과: 실시간 이상징후 탐지로 보안 사고 0건, 인프라 비용 35% 절감

1.6.5 ☒ AI 기반 인프라 자동화 플랫폼 (2024.09 ~ 현재)

개인 프로젝트 | AI-Powered Infrastructure Automation & Observability Platform

GitHub: github.com/qws941 | Live: <https://resume.jclee.me>

시스템 규모 & 아키텍처:

- 인프라: Rocky Linux 9.6, Hyper-V
- 프로젝트: 12개 프로덕션 애플리케이션 (blacklist, mcp, resume, safework, grafana, n8n 등)
- 컨테이너: 30개 Docker 컨테이너, 15개 운영 컨테이너 (Prometheus, Loki, Promtail, cAdvisor, Node Exporter)
- 모니터링: 중앙 집중식 Grafana Stack (Synology NAS), 99.5% 고가용성

기술스택 & 도구:

- AI/ML: Claude Code (Sonnet 4.5), MCP Protocol, GitHub Copilot
- 컨테이너: Docker, Docker Compose, Watchtower (자동 업데이트), Portainer API
- 모니터링: Grafana, Prometheus, Loki, Tempo, Splunk, cAdvisor, Node Exporter
- 언어: Python 3.9, Node.js 22, JavaScript/TypeScript, Shell Script
- CI/CD: GitHub Actions, Cloudflare Workers, Git-based automation
- 네트워크: Traefik (Reverse Proxy), NFS v3/v4 (Synology integration), Multi-host Docker

세부 프로젝트 컴포넌트:

1. ML Agent Selection System

- 목적: ML 기반 자동 에이전트 라우팅 시스템
- 기술스택: Python, Flask, Scikit-learn, PostgreSQL, MCP Servers
- 규모: 50개 스크립트 관리, Constitutional Framework
- 성과: AI 작업 효율 40% 향상, 자동 에이전트 라우팅으로 의사결정 시간 80% 단축
- Live: <http://127.0.0.1:5001>
- GitHub: github.com/qws941/claude

2. n8n Workflow Automation

- 목적: Self-hosted 워크플로우 자동화 플랫폼
- 기술스택: n8n, PostgreSQL, Redis, Docker
- 규모: 100개 템플릿, 50개 API 오케스트레이션
- 성과: 반복 작업 자동화로 월 200시간 절감, 워크플로우 재사용성 300% 향상
- Live: <https://n8n.jclee.me>
- GitHub: github.com/qws941/n8n

3. GitLab Enterprise Edition

- 목적: Self-hosted DevOps 플랫폼 및 Container Registry
- 기술스택: GitLab EE, PostgreSQL, Redis, Traefik
- 규모: 50개 CI/CD pipelines, 200개 Container 이미지, 자동 백업
- 성과: Private 코드 호스팅, 자동화된 CI/CD, 배포 시간 70% 단축
- Live: <https://gitlab.jclee.me>
- GitHub: github.com/qws941/claude/tree/main/app/gitlab

4. Nginx Airgap Configuration

- 목적: 폐쇄망 환경용 Nginx 설정 및 보안 강화
- 기술스택: Nginx, Airgap Deployment, Security Hardening
- 특징: 패키지 사전 준비, 오프라인 설치 지원
- 성과: 폐쇄망 환경에서 100% 자급 배포 가능, 보안 설정 표준화
- GitHub: github.com/qws941/nginx

5. Python Automation Framework

- 목적: 인프라 자동화 프레임워크
- 기술스택: Python, Ansible, Bash, Git Hooks
- 특징: 파일 거버넌스, AI 보상 시스템, 세션 연속성
- 성과: 인프라 운영 시간 60% 단축, 스크립트 재사용성 200% 향상
- GitHub: github.com/qws941/claude

6. Constitutional Governance System

- 목적: 파일 생성 쿼터 관리 및 구조 거버넌스
- 기술스택: Bash, Python, JSONL, Git Hooks
- 규모: 일일 100개 파일 쿼터, 유사도 감지, 자동 로깅
- 성과: 파일 중복 90% 감소, 프로젝트 구조 일관성 100% 유지
- GitHub: github.com/qws941/claude/blob/main/scripts/master-prevention-system.sh

7. AI Compensation Core

- 목적: AI 한계 보상 시스템
- 기술스택: Python, Pattern Detection, Multi-Model Validation
- 보상 영역: Context window, Hallucination 감지, Real-time data, Domain routing

- 성과: AI 오답률 70% 감소, 작업 신뢰도 95% 향상
- GitHub: github.com/qws941/claude/blob/main/scripts/ai-compensation-core.py

8. Ansible FortiManager Automation

- 목적: FortiManager 방화벽 정책 자동화 (Infrastructure as Code)
- 기술스택: Ansible, FortiManager API, Ansible Vault, Docker
- 규모: 200개 플레이북, fortinet.fortimanager collection
- 기능: 정책 조회/생성/수정, 백업/복원, 오브젝트 관리, Docker 배포 자동화
- 성과: 정책 배포 시간 90% 단축, 수동 오류 100% 제거
- GitHub: github.com/qws941/policy

9. NAS Infrastructure Deployment

- 목적: Synology NAS 인프라 자동 배포 시스템
- 기술스택: Bash, rsync, SSH, Docker Compose, Synology DSM
- 규모: 10개 서비스 (Grafana, Prometheus, Loki, AlertManager, GitLab, Traefik, Splunk, Promtail, Node Exporter)
- 기능: 원격 Docker 관리, 자동 rsync 동기화, 멀티 서비스 오케스트레이션
- 성과: 배포 자동화로 수동 작업 100% 제거, 인프라 동기화 시간 95% 단축
- GitHub: github.com/qws941/claude/tree/main/infra

핵심 아키텍처 설계:

1. Universal Observability Architecture

- 중앙 집중식 모니터링 (Synology NAS: grafana.jclee.me)
- 메트릭 수집: Prometheus, 500개 메트릭, Synology 통합
- 로그 수집: Promtail, Loki, Grafana 실시간 스트리밍 (일일 10GB)
- 컨테이너 메트릭: cAdvisor (8081) + Node Exporter (9101)
- 헬스체크: 모든 서비스 /health 엔드포인트 표준화

2. Multi-Host Docker Context System

- 로컬 Docker (localhost): blacklist, mcp, local-exporters
- Synology Docker (192.168.50.215): grafana, n8n, xwiki, file
- NFS 마운트: /home/jclee/app/{grafana,n8n,xwiki}, Synology 동기화
- .docker-context 파일 기반 자동 라우팅

3. AI-Driven Automation Framework

- SlashCommand 시스템 (50개 명령어)
- MCP 도구 생태계: 15개 도구 (filesystem, github, slack, tmux, n8n, sqlite, puppeteer)
- Constitutional AI 거버넌스 (CLAUDE.md: 자율 실행, 검증, 메타 학습)
- 자동화 스크립트: 100개 Bash scripts (보안, 모니터링, 배포, 테스트)

4. Production-Ready CI/CD Pipeline

- GitHub Actions: resume (Cloudflare Workers), blacklist (Docker)

- Watchtower: 자동 이미지 업데이트 및 무중단 재배포
- Git-based: 모든 변경사항 추적 가능, 자동 롤백 지원
- 테스트 자동화: Jest (유닛), Playwright (E2E), 커버리지 95%

프로젝트별 상세:

Resume Portfolio (Cloudflare Workers + Observability)

- 배포: <https://resume.jclee.me> (저지연 응답 <50ms, 글로벌 CDN)
- 기술스택: Cloudflare Workers, HTML/CSS, JSON-LD SEO, Grafana Loki 통합
- 인프라: GitLab (Primary, 192.168.50.215:2222) + GitHub (Mirror, CI/CD)
- CI/CD: GitHub Actions 자동 배포, 배포 타임스탬프 주입
- 모니터링:
 - Grafana Loki 실시간 로깅 (<https://grafana.jclee.me/loki>)
 - Prometheus 메트릭 수집 (/metrics 엔드포인트)
 - Web Vitals 추적 (LCP <2.5s, FID <100ms, CLS <0.1)
 - Health Check (/health): 배포 시각, 99.5% 가동률, 일일 10만 요청 처리
- 보안: CSP SHA-256 해시 (unsafe-inline 제거), HSTS, X-Frame-Options
- 테스트: 100% 테스트 커버리지, E2E 테스트 (Playwright)
- 성과: Lighthouse 100점 (Performance, Accessibility, SEO), Open Graph 소셜 미리보기
- 최신 배포: 2025-12-20T10:30:00Z

Blacklist (IP 블랙리스트 관리 시스템)

- 아키텍처: PostgreSQL, Redis, Flask, React (Frontend)
- 스케일: 일일 100만 IP 주소 실시간 관리
- 모니터링: Prometheus metrics (/metrics), Health check (/health)
- 배포: Multi-port (2542), Docker Compose, Traefik integration

MCP Platform (AI 도구 통합)

- 역할: Model Context Protocol 서버 통합 플랫폼
- 규모: 15개 MCP 서버, 50개 도구 (filesystem, github, slack, tmux, n8n)
- WebUI: Node.js, Nginx reverse proxy
- 성과: AI 작업 효율 50% 향상, 도구 통합 복잡성 80% 감소

Local Exporters (모니터링 스택)

- 구성: Prometheus, Node Exporter, cAdvisor, Promtail
- 메트릭: 시스템 (CPU, RAM, Disk), 컨테이너 (Docker stats), 로그 (Loki)
- 중앙 통합: Synology Grafana (192.168.50.215)

Splunk Demo (로그 분석)

- 규모: 일일 50GB 이벤트 처리

- 포트: 8000 (WebUI), 8088 (HEC), 9997 (Forwarder)
- 용도: 보안 이벤트 중앙 집중 분석, FortiNet 통합

운영 성과 (2024.09 ~ 현재):

- 자동화: 반복 작업 90% 자동화, 월 200시간 절감
- 안정성: MTTR 15분 → 2분 (87% 개선), MTBF 720시간
- 가시성: 15개 통합 대시보드, 모든 서비스 실시간 모니터링
- 테스트: Jest + Playwright 통합, 95% 커버리지 달성
- 보안: SELinux + Firewall 구성, 보안 사고 0건
- 비용: 로컬 + Synology 하이브리드로 클라우드 비용 100% 절감

기술적 하이라이트:

- Worker 생성 자동화 (generate-worker.js)
- ROUTES 객체 패턴 (10개 라우트)
- Integration 테스트 (100% 커버리지)
- Constitutional AI (자율 실행 + 검증)
- Docker Context Auto-routing (3개 환경)

1.7 기술 스택

1.7.1 보안 솔루션

- 네트워크 보안: 방화벽, DDoS, IPS/IDS, WAF
- 엔드포인트: NAC, DLP, EDR/EPP, MDM, APT
- 접근제어: 서버/DB 접근제어, SSL VPN, IPSec, SSL 복호화
- 모니터링: SIEM, SOAR

1.7.2 클라우드 및 가상화

- AWS: EC2, VPC, IAM, S3, CloudTrail, GuardDuty, Route53
- 가상화: VMware vSphere, NSX-T, Hyper-V
- 컨테이너: Docker, Kubernetes, Helm

1.7.3 자동화 및 개발

- Languages: Python, Shell Script, PowerShell, Node.js, TypeScript, JavaScript
- IaC: Ansible, Terraform, CloudFormation
- CI/CD: Jenkins, GitLab CI, GitHub Actions, Watchtower
- 모니터링: Prometheus, Grafana, Loki, ELK Stack, Tempo, Splunk

1.7.4 AI/ML 및 자동화

- AI 도구: Claude Code, GitHub Copilot, ChatGPT API
- MCP 프로토콜: 서버 통합 (filesystem, github, brave-search, memory, tmux 등)
- 자동화 프레임워크: Custom SlashCommand 시스템
- 관찰성: Universal Observability 아키텍처 (Grafana 중심)

1.7.5 컨테이너 및 오케스트레이션

- 컨테이너 플랫폼: Docker, Portainer API, Docker Compose
- 레지스트리: Private Docker Registry (registry.jclee.me)
- 배포 전략: Multi-Port Deployment, Blue-Green, Canary
- 자동화: Watchtower 기반 자동 업데이트, 무중단 배포

1.7.6 네트워크

- Routing/Switching: OSPF, BGP, VLAN, VxLAN
- Load Balancing: F5, HAProxy, Nginx
- SDN: VMware NSX-T, OpenFlow

1.8 자격증

자격증명	발급기관	취득일
CCNP	Cisco Systems	2020.08
RHCSA	Red Hat	2019.01
CompTIA Linux+	CompTIA	2019.02
LPIC Level 1	Linux Professional Institute	2019.02
사무자동화산업기사	한국산업인력공단	2019.12
리눅스마스터 2급	한국정보통신진흥협회	2019.01

최종 업데이트: 2025년 12월 20일