AWS Well-Architected 참조 아키텍처의 국내 클라우드 환경 투영과 관측가능성 평가 프레임워크

이은진[1], 박주원[1], 권수빈[1], 표자연[1], 박기웅[2†]
[1]세종대학교 정보보호학과 학부생
[2]세종대학교 정보보호학과 교수
22011760@sju.ac.kr park21@sju.ac.kr, 22011775@sju.ac.kr, 23011727@sju.ac.kr,
woongbak@sejong.ac.kr

An Observability Assessment Framework for Domestic Cloud Platforms Based on AWS Well-Architected Reference Architecture

Eun-jin Lee[1], Joowon Park[1], Soo-Bin Kwon[1], Jayeon Pyo[1], Ki-Woong Park[2]
[1,2]Dept. of Computer and Information Security, Se-jong University

요 약

본 연구는 AWS Well-Architected Framework를 기준으로 국내 주요 클라우드 플랫폼의 보안 관측 가능성 커버리지를 비교·분석하였다. 이를 위해 Security Pillar와 Operational Excellence Pillar의 OPS04에서 핵심 관측 역량을 추출하고, 데이터 수집, 서비스 간 상관관계 분석, 시각화 및 탐색, 이상 탐지 및 자동 대응, 트레이싱 커버리지, 문서 및 가이드 커버리지의 6개 비교 축과 23개 항목을 구성하였다. AWS를 기준점으로 평가한 결과, 국내 CSP는 기초적인 수집 기능은 갖추고 있으나 전반적으로 제한적인 커버리지를 보였다. 특히 트레이싱 기능과 공식 운영 가이드의 부족은 사고 원인 식별과 대응 효율성 저하로 이어질 수 있는 한계로 확인되었다.

1. 서론

클라우드 환경의 확산과 함께 보안 위협 또한 증가하고 있다. KISA에 따르면 2025년 국내 침해사고 신고 건수는 2,383건으로 전년 대비 26.3% 증가하여 역대 최다를 기록하였다[1]. 같은 해 국내 주요 기업에서 대규모 개인정보 유출 사고가 연이어 발생하면서 클라우드 환경에서의 보안 운영 중요성이 더욱 부각되었다.

다양한 보안 솔루션의 도입만으로는 침해를 효과적으로 방지하기 어렵다. 관련 사례들은 로그 수집, 위협 탐지, 대응 체계가 유기적으로 연계되지 않을 경우 보안 운영의 실효성이 저하될 수 있음을 보여주며, 이는 보안 관측 가능성의 필요성을 시사한다.

이에 본 논문은 AWS Well-Architected Framework Security Pillar(OPS04)를 기준으로 [2-4] 국내 주요 3개 클라우드 플랫폼의 보안 관측 가능성을 6개 축, 23개 항목에서 비교 및 분석하고 시사점을 도출한다.

† 교신저자: 박기웅 (세종대학교 정보보호학과 교수)

2. 배경 및 관련 연구

2.1 보안 관측 가능성

관측 가능성(Observability)은 시스템의 외부 출력으로부터 내부 상태를 추론하는 능력을 의미하며, 일반적으로 로그, 메트릭, 트레이스를 핵심 신호로 한다. 보안 관측 가능성은 이를 보안 운영에 적용한 개념으로, 단순한 로그 수집을 넘어 보안 이벤트의 탐지, 상관관계 분석, 원인 규명, 대응 연계까지 포함하는 통합적 운영 역량으로 이해할 수 있다.

2.2 관련 연구

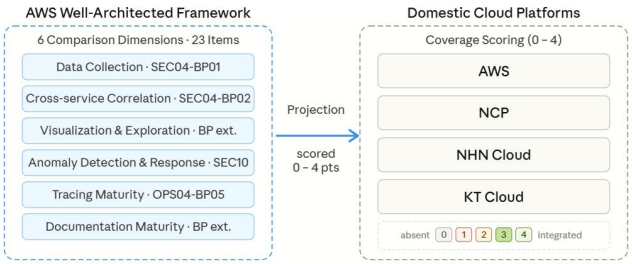
기존 연구는 주로 두 방향에서 수행되어 왔다. 하나는 observability와 분산 시스템 모니터링 관점에서 로그, 메트릭, 트레이스, 분산 추적의 중요성을 다룬 연구이며, 다른 하나는 MITRE ATT&CK 기반 위협 탐지 및 대응 전략에 초점을 둔 연구이다. 그러나 이러한 연구들은 플랫폼 수준에서 보안 관측 가능성의 지원 범위를 비교·평가하는 데에는 한계가 있다. 이에 본 연구는 AWS Well-Architected Framework를 기준으로 국내 클라우드 플랫폼의 보안 관측 가능성을 동일한 틀에서 비교한다는 점에서

차별성을 가진다.

3. 연구 방법론

3.1 비교 프레임워크 설계

본 연구는 AWS Well-Architected Framework의 Security Pillar와 Operational Excellence Pillar의 OPS04 항목을 바탕으로 [2-4] 국내 클라우드 플랫폼의 보안 관측 가능성 커버리지를 비교하기 위한 프레임워크를 설계하였다. 관련 Best Practice에서 요구하는 핵심 관측 역량을 추출하고, 실무 활용성과 문서 기반 분석의 특성을 반영하여 총 6개의 비교 축을 도출하였다.



(그림 1) 프레임워크 설계

첫째, 데이터 수집 축은 SEC04-BP01을 바탕으로 설정하였다[3]. 이는 로그, 메트릭, 이벤트 등 관측 데이터의 수집 범위와 수집 편의성을 평가하기 위한 것으로, 보안 관측 가능성의 기초 계측 역량에 해당한다.

둘째, 서비스 간 상관관계 분석 축은 SEC04-BP02를 참고하여 구성하였다[3]. 이는 개별 로그만으로 파악하기 어려운 서비스 간 연관성, 이상 징후의 발생 맥락, 그리고 원인 지점 식별 역량을 평가하기 위한 것이다.

셋째, 시각화 및 탐색 축은 수집된 관측 데이터를 실무자가 신속하게 해석하고 이상 징후를 인지할 수 있는지를 평가하기 위해 포함하였다[3]. 이 축은 관련 Best Practice의 요구사항을 실무 활용 관점에서 확장한 보완적 평가 기준이다.

넷째, 이상 탐지 및 자동 대응 축은 SEC04-BP03, SEC04-BP04 및 SEC10을 반영하여 설정하였다[3]. 이는 탐지 결과가 경보 발생에 그치는지, 또는 실제 대응 절차와 자동화된 조치로 연계되는지를 평가하기 위한 것이다.

다섯째, 트레이싱 성숙도 축은 OPS04-BP05를 바탕으로 포함하였다[4]. 이는 분산 환경 및 마이크로서비스 구조에서 요청 흐름과 서비스 의존관계를 추적할 수 있는 역량을 평가하기 위한 것이다.

여섯째, 문서 및 가이드 성숙도 축은 기능 제공 여부와는 별도로, 사용자가 해당 기능을 실제 환경에 적절히 설계·운영할 수 있도록 지원하는 공식 문서와 참조 가이드의 수준을 평가하기 위해 추가하였다[4]. 이 축은 문서 기반 비교 연구의 특성과 실무적 활용 가능성을 함께 반영한 기준이다.

3.2 커버리지 평가 기준

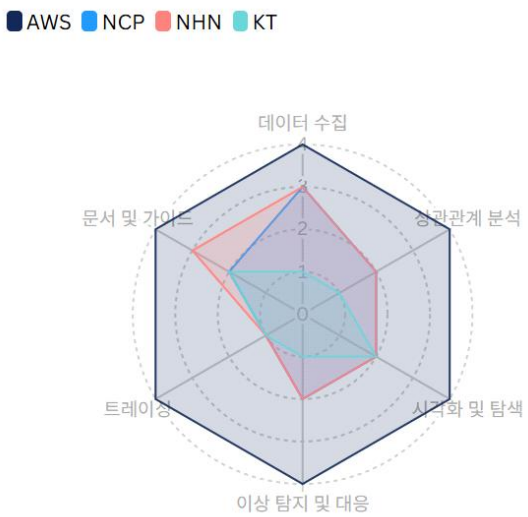
각 항목은 표 1의 0~4점 5단계로 평가하였다. 0점은 기능 자체가 없거나 문서에서 확인 불가한 경우, 4점은 자동화, 상관관계 분석, 참조 가이드까지 포함한 고도화된 수준을 의미한다.

<표 1> 커버리지 평가 기준

점수	커버리지 수준	평가 기준
0점	부재	해당 기능 또는 지원 체계가 제공되지 않는 경우
1점	제한	개별 기능은 제한적으로 제공되나, 수집·활용 범위가 협소하고 연계성이 부족한 경우
2점	기초	기본 기능은 제공되나 서비스 간 통합, 상관관계 분석, 자동화 수준이 제한적인 경우
3점	확장	기능 간 연계와 운영 활용이 가능하며 시각화, 탐색, 경보 연계 등 실무 활용성이 확보된 경우
4점	통합	자동화, 상관관계 분석, 분산 추적, 참조 가이드 및 모범 사례까지 포함한 통합 운영 체계가 갖춰진 경우

4. 분석 결과

4.1 커버리지 비교 매트릭스



(그림 2) 커버리지 비교 그래프

4.2 커버리지 비교 결과

국내 CSP 3사는 인프라 구축 역량 대비 사고 추적을 위한 보안 관측 설계 자산이 전반적으로 미비하다. 특히 마이크로서비스 간 요청 흐름을 시각화하는 트레이싱 기술은 3사 모두 공백 상태로 확인되어 사고 전파 경로 파악에 한계가 존재한다.

NCP와 NHN Cloud는 통합 로그 플랫폼을 통해 1년 내외의 장기 데이터를 보존하는 등 기초 수집 역량은 양호한 수준이다. 그러나 수집된 데이터를 사고 맥락에 맞게 연결하는 상관분석 도구가 부족하고, 머신러닝 기반 탐지나 자동화된 대응 시나리오(Playbook)의 커버리지가 낮아 보안 운영자의 수동 분석 의존도가 매우 높다.

KT Cloud는 분석 대상 중 가장 낮은 커버리지를 보였다. 서버 감사 로그 및 네트워크 흐름 로그의 수집 가이드가 부재하며, 특히 7일의 짧은 데이터 보존 주기는 사후 포렌식을 불가능하게 만드는 치명적 결함이다. 또한, 이상 탐지 시 공격을 즉각 차단할 수 있는 API 기반 자동 대응 인터페이스가 마련되어 있지 않아 능동적 보안 관측에 큰 제약이 있다.

다만, 본 비교는 AWS Well-Architected Framework를 평가 기준으로 삼고 있어 AWS 생태계에 최적화된 구조적 특성상 국내 CSP에 불리하게 작용할 수 있음을 고려해야 한다[2].

I. 결론

본 연구는 AWS Well-Architected Framework를 기준으로 국내 주요 클라우드 플랫폼의 보안 관측 가능성 커버리지를 6개 축에서 비교·분석하였다. 분석 결과, 국내 CSP는 기초적인 로그 수집 역량은 확보하고 있으나, 상관관계 분석, 분산 추적, 자동 대응 연계 측면에서는 전반적으로 미흡한 수준을 보였다. 특히 트레이싱 기능의 부재와 문서·가이드 자산의 한계는 사고 원인 식별과 신속한 대응을 제약하는 주요 요인으로 확인되었다. 이는 국내 클라우드 플랫폼이 단순 인프라 제공을 넘어, 보안 관측 가능성을 중심으로 한 통합 운영 역량을 강화할 필요가 있음을 시사한다.

Acknowledgement

본 연구은 과학기술정보통신부의 재원으로 정보통신기획평가원(IITP)의 정보보호핵심원천기술개발(Project No. RS-2026-25519773, 30%; RS-2024-00438551, 10%), 실감콘텐츠핵심기술개발(Project No. RS-2023-00228996, 20%), 대학ICT연구센터(ITRC) (Project No. ,10% IITP-2026-RS-2021-II211816, 10%), 한국연구재단(NRF) 핵심연구사업(Project No. RS-2026-25481431 30%)의 지원을 받아 수행된 연구임.

참고문헌

[1] 한국인터넷진흥원, 2025년 하반기 사이버 위협 동향 보고서, 한국인터넷진흥원, 2026.

[2] Amazon Web Services, AWS Well-Architected Framework, Amazon Web Services, 2024.

[3] Amazon Web Services, AWS Well-Architected Framework: Security Pillar, Amazon Web Services, 2024.

[4] Amazon Web Services, AWS Well-Architected Framework: Operational Excellence Pillar, Amazon Web Services, 2024.