AWS와 국내 CSP의 서비스 비교를 통한 국내 CSP 침해대응 가시성 및 추적성 분석

정기연[1], 양지원[2], 김세현[3], 김도영[4], 박기웅[5*]
[1]고려대학교 바이오의공학부 학부생
[2]중앙대학교 산업보안학과 학부생
[3]중앙대학교 역사학과 학부생
[4]세종대학교 정보보호학과 학부생
[5]세종대학교 정보보호학과 교수
jhhjgy2@korea.ac.kr, start3127@cau.ac.kr, michael0903@cau.ac.kr,
dgreezero01@sejong.ac.kr, woongbak@sejong.ac.kr

Analysis of Domestic CSP Incident Response Visibility and Traceability through a Comparison of AWS and Domestic CSP Services

Ki-Yeon Jeong[1], Ji-Won Yang[2], Se-Hyeon Kim[3], Do-Yeong Gim[4], Ki-Woong Park[5*]
[1]School of Biomedical Engineering, Korea University
[2]Dept. of Industrial Security, Chung-Ang University
[3]Dept. of History, Chung-Ang University
[4]Dept. of Computer and Information Security, Sejong University
[5]Dept. of Computer and Information Security, Sejong University

요 약

본 연구는 클라우드 침해사고 대응의 핵심 요건인 가시성(Visibility)과 추적성(Traceability)을 제고하기 위해, AWS와 국내 주요 CSP(Naver Cloud, 이하 Naver; NHN Cloud, 이하 NHN; kt Cloud, 이하 kt; Gabia Cloud, 이하 Gabia)의 보안·모니터링 관련 서비스를 체계적으로 비교·분석하였다. ISMS-P, 개인정보보호법, NIST-SP를 준거로 비교 기준을 도출하고, 각 CSP의 로그·보안 서비스가 해당 기준을 충족하는 수준과 AWS 대비 미흡점을 진단하였다. 분석 결과, 종합 만족 수준은 AWS, Naver, NHN, kt, Gabia 순으로 높았다. 주요 격차 요인은 ① 감사 로그의 포괄성, ② 비용 모니터링의 준실시간성 및 이상탐지, ③ 다계층 자동 보안 이벤트 모니터링, ④ 서비스 간 통신 추적의 언어 지원 범위, ⑤ WORM·규정준수 모드 등 증거보전 기능, ⑥ 에스컬레이션 에서 나타났다. 이러한 분석을 통해 국내 CSP의 취약 지점을 확인하고, 향후 보완이 필요한 과제를 제시하였다.

1. 서론

클라우드 환경에서 침해대응의 핵심은 로그 확보를 통한 가시성·추적성 강화가 중요하다. 한편, 세계적으로 높은 점유율을 보이는 AWS는 체계적 로그 제공으로 가시성·추적성을 평가할 수 있는 대표적 기준이 되지만, 국내 CSP를 이것에 비교한 연구는 아직 제한적이다. 이에 본 연구는 AWS와 국내 주요 CSP (Naver, NHN, kt, Gabia) 의 모니터링·보안 서비스를 비교해 가시성·추적성의 수준 차이를 진단하고 개선 방향을 시사하고자 한다.

2. 연구 방법

ISMS-P·개인정보보호법·NIST-SP로부터 도출한 비교항목을 기준으로, AWS, Naver, NHN, kt, Gabia의 보안·모니터링 서비스가 각 항목을 만족하는 정도를 조사하였다. 이후 각 CSP의 충족 수준과 최고 수준 대비 미흡점을 분석하였다.

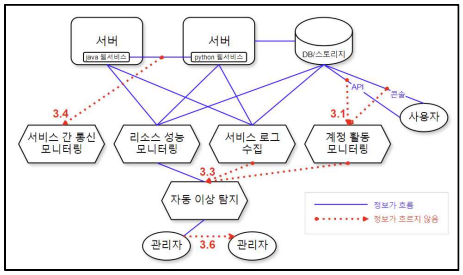
3. 서비스 비교 결과 및 문제점 도출

각 CSP의 보안 및 모니터링 관련 서비스에 대해 비교항목을 기준으로 만족 수준을 분석한 결과, 종합적인 만족 수준은 AWS, Naver, NHN, kt, Gabia 순서대로 높은 것으로 나타났다.

<표 1> CSP의 비교항목 만족 수준 분석 표.

비교항목	AWS	Naver	NHN	kt	Gabia
1. 감사 로그 관리	○	○	△	△	×
2. 리소스 모니터링	○	○	○	○	○
3. 비용 모니터링	○	△	△	×	×
4. 보안 이벤트 모니터링	○	△	△	△	△
5. 트래픽 모니터링	○	○	○	○	○
6. 서비스 간 통신 모니터링	○	○	○	△	△
7. 로그 분석	○	○	○	○	○
8. 데이터 보존 및 아카이빙	○	○	○	△	△
9. 알림 및 에스컬레이션	○	△	△	△	△

○: 거의 만족 / △: 일부만 만족 / ×: 거의 불만족



(그림 1) 3.1, 3.3, 3.4, 3.6절에서 언급된 국내 CSP의 미흡점이 포함된 클라우드 구성도.
특정 CSP에 대한 설명이 아니라 미흡한 경우에 대한 예시이다.

아래와 같이, 국내 CSP의 미흡점이 침해 대응의 가시성과 추적성에 주는 문제를 분석하고 개선 방안을 제시하였다.

3.1. 감사 로그 관리

AWS는 CloudTrail로 계정·서비스 API, VPC Flow Logs로 네트워크, S3 데이터 이벤트로 객체 접근을 기록하며, RDS/Aurora는 엔진별 감사 기능을 지원한다. Naver는 Activity Tracer·Object Storage Access Logging·Flow Log를 제공하고 DB 감사는 엔진/옵션 의존적이다. NHN은 CloudTrail·Flow Log·DB 감사 플러그인을 제공하되 서비스별 커버리지가 상이하다. KT는 Watch 기반의 지표·이벤트 관제를 제공한다. Gabia는 통합 모니터링으로 서버·DB 접속 관제를 제공한다.[1][2][3][4][5]

3.2. 비용 모니터링

AWS는 Budgets·Cost Explorer·Cost Anomaly Detection으로 예산 관리와 비용 이상 탐지·알림을 제공하며 데이터는 국내 CSP와 달리 일중 다회 갱신된다. Naver는 예산 알림과 비용 리포트를 제공한다. NHN은 예산/청구 관리와 알림을 제공한다. KT는 포털 요금/이용내역 조회와 Watch 지표 알람을 제공한다. Gabia는 청구 리포트와 모니터링을 제공한다.

3.3. 보안 이벤트 모니터링

국내 CSP에서는 다계층+자동탐지를 동시에 충족하는 서비스를 찾기 어려웠다. 대개는 소스별 자동탐지이거나 관제 기반 다계층 탐지에 그친다.

3.4. 서비스 간 통신 모니터링

통신 모니터링 기능이 지원되는 언어는 AWS에서는 go·java·js·python·.net으로 5개, Naver와 NHN에서는 java·python·.net·php으로 4개, kt와 Gabia에서는 java 1개였다. 따라서 지원되지 않는 언어로 작성된 서비스에서 공격자가 권한 상승이나 내부 DB 접근을 시도하는 경우에는 공격 추적 및 근본 원인 분석이 어려워질 수 있다.

3.5. 데이터 보존 및 아카이빙

WORM(Write-Once, Read-Many) 기능은 AWS, Naver, NHN만 지원하며, 특히 AWS는 루트 사용자를 포함한 어떤 사용자도 데이터를 삭제할 수 없는 '규정 준수 모드'와 특정 관리자는 예외를 허용하는 '거버넌스 모드'의 2가지 옵션을 모두 리전에서 제공한다. 반면, Naver는 한국 리전에서는 규정 준수 모드를 제공하지 않으며 일본 리전에서만 제공한다. NHN는 단일 잠금 모드만 제공하며, 루트 사용자에 의한 무력화 가능 여부가 불명확하다. kt와 Gabia는 네이티브 객체 잠금 기능 자체가 부재하다. 이러한 기능적 격차는 공격자가 루트 권한 탈취 시 로그 등의 핵심 증거를 인멸할 가능성을 열어두므로, 침해 대응의 법적 증명력과 추적성을 약화시킨다.

3.6. 알림 및 에스컬레이션

AWS는 Incident Manager를 통해 '1차 담당자가 5분 내 미응답 시 2차 담당자 호출'과 같은 다단계·시간 기반의 자동 에스컬레이션 계획 기능을 제공한다. 반면 Naver는 동일 담당자 그룹에 반복적으로 알림을 보내는 리마인드 기능만을 지원하며, NHN, kt, Gabia의 모니터링 서비스는 정적인 단일 수신자 그룹으로의 알림 전송에 그친다. 이로 인해 알림 누락 시 MTTD·MTTR 증가를 초래할 수 있다.

4. 결론

본 연구는 AWS와 국내 CSP를 비교·분석하여 국내 CSP의 미흡한 지점을 규명하였으며, 이를 개선한다면 침해대응 측면에서 국내 CSP의 보안 수준은 한층 높아질 것이다. 향후 연구에서는 실제 공격 시나리오를 기반으로 한 실증적 검증이 요구된다.

참고문헌

[1] Amazon Web Services 공식 문서. https://docs.aws.amazon.com/.
[2] NAVER Cloud Platform 공식 문서.https://guide.ncloud-docs.com/docs/home.
[3] KT Cloud 공식 문서. https://manual.cloud.kt.com/kt/education-edubasic-edu_ess_1.
[4] NHN Cloud 공식 문서. https://docs.nhncloud.com/ko/nhncloud/ko/overview/.
[5] 가비아 클라우드 공식 문서. https://customer.gabia.com/manual/cloud/21981.