Cloud Sentinel: 국내 클라우드 침해사고 대응을 위한 초동 로그 분석 체계

정미정 [1], 이유진 [1], 이동현 [2], 박기웅 [3]
[1] 서울여자대학교 정보보호학과 학부생
[2] 고려대학교 SW·AI 융합대학원 소프트웨어 보안학과 석사과정
[3] 세종대학교 정보보호학과 교수

notyetchoose@swu.ac.kr, leeyujin02@swu.ac.kr, mmostory@korea.ac.kr, woongbak@sejong.ac.kr

Cloud Sentinel: Log-Centric Early Response Framework for Cloud Security Incidents

Mi-Jeong Jeong[1], Yu-Jin Lee [1], Dong-Hyun Lee[2], Ki-Woong Park[3]
[1]Dept. of Information Security, Seoul-Women University (Undergraduate Student)
[2]Dept. of Software Security, Korea University (Graduate Student)
[3]Dept. of Computer and Information Security, Sejong University (Professor)

요 약

클라우드는 계정 접근 및 권한 탈취, 1-day·N-day 취약점, 설정 오류와 같은 위협들에 노출되고 있으며, 공격자들은 공격을 통해 수백 달러 이상의 수익을 획득하고 있다. 클라우드 환경에서 발생하는 보안 사고는 서비스 확산성과 다계층 구조로 인해 피해가 단기간에 급격히 확산할 수 있으므로, 초동 조치는 사고 대응의 효과성을 좌우하는 핵심 과정이다. 신속하고 체계적인 초동 분석은 사고 원인 규명과 피해 최소화, 그리고 후속 대응 전략 수립의 기초를 제공한다. 기존 침해 대응 안내서들은 주로 AWS, Azure 등 해외 클라우드 서비스를 중심으로 구성되어 있어, 국내 클라우드 환경의 고유한 특성과 서비스 구조를 충분히 반영하지 못하는 한계가 있다. 본 연구는 네이버 클라우드 플랫폼 특화의 침해사고 메뉴얼을 제안하고자 한다.

1. 서론

최근 클라우드 보안 사고 사례가 많아지면서, 클라우드 침해사고 대응 프로세스가 요구되고 있다[1]. 기존의 정보통신분야 침해사고 대응 안내서(개정본)[2]에서 웹 기반 침해 사고에 대한 수집 방안을 제시하고 있으나, 클라우드 환경은 포함하지 않고 있다. 또한 클라우드 보안 가이드[3]에서 계정관리, 네트워크 보안 등의 보안 설정 방법을 제공하고 있으나, 침해사고 발생 시 메뉴얼이 없어 선별 수집할 로그를 직접 찾아야 한다. 이에 따라 초동 분석에 많이 시간이 소요되고, 유실되는 로그가 존재한다.

본 논문에서는 글로벌 보안 단체 CSA 에서 선정한 클라우드 위협 Top11[4]을 기반으로 실제 침해사고를 분류하고, 사고 발생 시 공통 점검 사항을 바탕으로 네이버 클라우드 플랫폼(NCP)에서 우선으로 확인해야 할 로그를 체계적으로 제안하고자 한다. 이를 통해 초동 분석 시간을 단축하고, 국내 클라우드 환경에 특화된 실효성 있는 침해사고 대응 방안을 제시하여 관련 분야의 실무 발전에 이바지하고자 한다.

2. 클라우드 침해사고 사례

클라우드 계정 및 접근 권한 탈취 사례로는 2024 년 말 보고된 Snowflake 사건이 대표적이다. 공격자(UNC5537)는 Infostealer 를 통해 사전에 탈취한 계정 자격 증명을 사용해 수백 개의 Snowflake 고객사를 공격하고, 200 만 달러 이상의 수익을 획득했다. [5]

1-Day, N-day 취약점 사례로는 2025 년 Oracle Cloud 에서 CVE-2021-35587 패치가 적용되지 않은 점을 ”rose87168”이라는 해커가 악용하여 약 600 만 건의 데이터가 유출된 사건이 있다. [6]

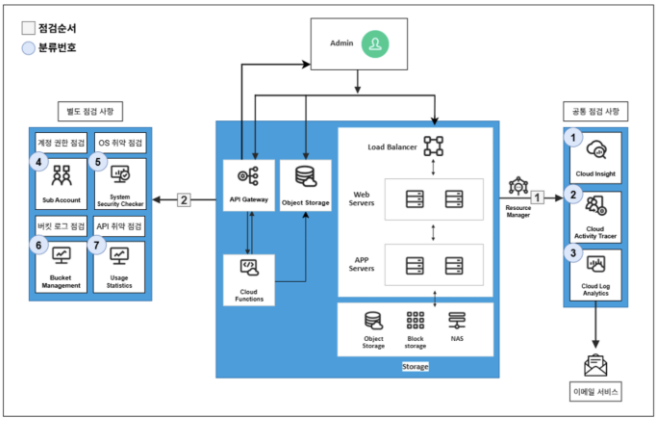
설정(구성) 오류의 사례로는 2023 년 Football Australia 의 사건이 있다. 해당 기관은 웹 소스 코드에 AWS 액세스 키를 하드 코딩하고, 인증이 설정되지 않은 S3 버킷을 통해 개인 정보가 노출되어 약 37 만 달러 이상의 피해를 입었다. [4]

앞선 클라우드 침해사고 사례들은 공격 유형의 다양성과 피해 규모의 심각성을 보여준다. 계정 탈취, 취약점 악용, 설정 오류 등 서로 다른 원인에도 불구하고 모두 조기 탐지의 어려움과 광범위한 영향이라는 공통된 특징을 나타내고 있어, 포괄적인 침해 대응 체계 구축의 중요성을 시사한다.

3. 침해사고 유형 및 초동 분석

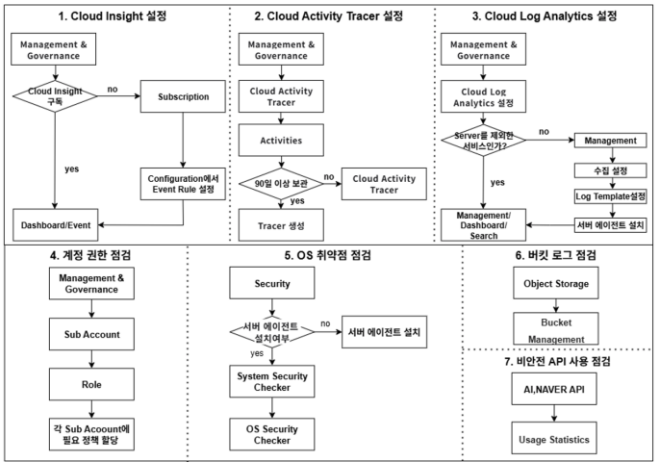
2장의 침해사고 유형이 여전히 심각한 위험으로 남아있다. 이에 CSA 2025 Top 11에서 총 6가지 침해사고 유형을 선별 후 초동 분석 방안을 제안한다.[7]

침해사고가 발생할 수 있는 유형은 다음과 같다. 첫째, 데이터 유출이나 서비스 중단이 발생할 수 있는 설정 오류 및 변경 관리 부실, 둘째, 시스템 변조와 악성 리소스 생성이 발생할 수 있는 계정 및 접근 권한 관리 미흡, 셋째, 안전하지 않은 소프트웨어 개발 경로, 넷째, 권한 상승이 발생할 수 있는 시스템 취약점 방치, 다섯째, 안전하지 않은 API 및 인터페이스, 여섯째, 민감 데이터나 서비스를 무단으로 이용이 발생할 수 있는 인증 없는 리소스 공유가 있다.



(그림 1) 침해사고 초동 분석 프레임워크

(그림 1)에서 정리된 바와 같이 침해사고 Cloud Activity Tracer, Cloud Log Analytics, Cloud Insight 서비스를 통해 통합적인 로그 점검을 수행한다. 또한 침해 사고 유형에 따라 Sub Account, System Security Checker, Bucket Management 에 대한 세부 점검 사항을 별도로 제안한다. 위의 프레임워크는 NCP 에서 제공하는 아이콘과 아키텍처를 활용한다.



(그림 2) NCP 서비스 로그 설정 확인 방법

NCP 로그 확인을 위해서는 사전 설정이 필수적으로 요구되며 로그 확인이 불가능한 경우 (그림2)를 통해 로그 설정의 적절성을 검증해야 한다.

침해사고 발생 유형	Cloud Analytics	Cloud Insight	Cloud Activity Tracer	OS Security Checker	Sub Account	Object Storage	API Usage Statistics
설정 오류 및 변경 관리 부실	O	O	O	X	X	O	X
계정 및 접근 권한 관리 미흡	O	O	O	O	O	O	X
안전하지 않은 소프트웨어 개발 경로	O	O	O	O	O	X	X
시스템 취약점 방치	O	O	O	X	O	X	X
안전하지 않은 API 및 인터페이스	O	O	O	X	O	X	O
인증없는 리소스 공유	O	O	O	X	O	X	X

(표 1) 침해사고 유형 별 NCP 서비스

침해 사고 발생시 유형별로 즉각적으로 확인해야 할 NCP 서비스는 (표 1)과 같다.

4. 결론 및 향후 연구

본 연구는 클라우드에서 침해사고 발생 시 초동 분석을 위한 가이드라인을 제안한다. CSA 2025 Top 11로 선정된 클라우드의 대표적인 6가지의 침해 사고에서 필요한 핵심 점검 항목을 설정한다. 이후 사건별 확인 경로를 로그 중심으로 분석하여 표와 다이어그램 형태로 표현한다. 최종적으로 NCP 환경에서 초동 분석 시 활용 가능한 국내 클라우드 침해사고 대응 가이드 방향성을 제안한다. 본 연구에서 제시한 분석 프레임워크는 국내 클라우드 환경을 사용하는 회사의 담당자들이 즉각적으로 활용할 수 있다. 또한 CSIRT Framework의 Log and Sensor Management와 Correlation 서비스에 해당하므로 국제적으로도 활용성이 높다. 향후 연구에서는 실제 침해사고 시나리오 기반의 실증 평가를 통해 제안 프레임워크의 실무 적용 가능성을 검증할 예정이다.

참고문헌

[1] Kim Sun-ae, “Two-thirds of cloud security breaches lack a clear incident response process”: https://www.datanet.co.kr/news/articleView.html? Idxno=193652, (accessed Sep. 12. 2025)

[2] KISA. (2025). 정보통신분야 침해사고 대응 안내서 (개정본) [PDF].

[3] NCP, “Naver Cloud Platform Security Guide”: https://www.ncloud.com/intro/securtiyNotice/materials, (accessed Sep. 12. 2025)

[4] CSA. (2025). Top-Threats-to-Cloud-Computing-Deep-Dive-2025 [PDF].

[5] Google Cloud, “UNC5537 Targets Snowflake Customer Instances for Data Theft and Extortion”: https://cloud.google.com/blog/topics/threat-intelligence/unc5537-snowflake-data-Theft-extortion?h1=en, (accessed Sep. 12. 2025)

[6] CloudSEK, “The Biggest Supply Chain Hack Of 2025: 6M Records Exfiltrated from Oracle Cloud affecting over 140K Tenants”: https://www.cloudsek.com/blog/the-biggest-supply-chain-hack-of-2025-6m-records-for-sale-exfiltrated-from-oracle-cloud-affecting-over-140k-tenants, (accessed Sep. 12. 2025)

[7] tenable. (2025). Tenable 클라우드 보안 위험 보고서 2025 [PDF].