클라우드 침해사고 초동대응에서의 실무적 난해도 서베이 및 분석

이지호*, 김병우*, 이근형*, 최진규*, 박기웅†

, † 세종대학교 정보보호학과(학부생, 교수†)

A Survey and Analysis of Practical Difficulties in Initial Incident Response for Cloud Environments

Jiho Lee*, Byungwoo Kim*, Geunhyeong Lee*, Jingyu Choi*, Giwoong Park†

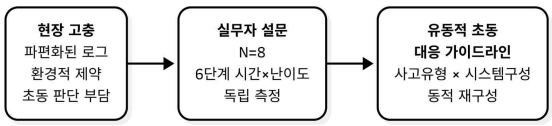
, † Sejong University(Undergraduate student, Professor†)

요 약

클라우드 환경의 복잡성이 증가함에 따라 침해사고 대응 현장에서는 CSP별로 상이한 로그 구조, 제한된 보존 기간, 파편화된 접근 권한 등 기술 외적 제약이 주요 병목으로 작용하고 있다. 그러나 기존의 대응 안내서와 플레이북은 정적 절차 기술에 머물러 있어, 현장 대응자가 실제로 어느 단계에서 어떤 부담을 겪는지에 대한 실증적 조사는 부족하다. 본 연구는 국내 클라우드 침해사고 대응 실무자 8명을 대상으로 침해사고 대응 6단계의 소요시간과 체감 난이도를 독립적으로 측정하는 설문을 수행하였다. 분석 결과, 인과 규명 및 복구 단계에 부담이 집중되고, 로그 환경의 파편성이 공통적으로 지적되었으며, 실무자들은 고난이도 작업 자체보다 그 선행 정보 정리의 자동화를 더 우선 요구함이 확인되었다. 본 연구는 이를 바탕으로 사고 유형과 시스템 구성에 따라 동적으로 재구성되는 유동적 초동 대응 가이드라인의 필요성을 제기한다.

I. 서론

클라우드 서비스의 확산과 함께 침해사고는 다수의 CSP와 관리 주체가 교차하는 복합적 형태로 변화하고 있으며[1], 현장 대응자는 CSP별로 상이한 로그 구조, 제한된 보존 기간, 파편화된 접근 권한 등 기술 외적 제약 속에서 초동 대응을 수행해야 한다. KISA와 CISA 등이 발간한 침해사고 대응 안내서[2,3]는 대체로 정적 절차 기술에 머물러 있어 CSP·시스템 구성·사고 유형의 조합에 따라 달라지는 현장 상황을 반영하기 어렵고, 현장 대응자가 실제로 어느 단계에서 어떤 부담을 겪는지에 대한 실무자 관점의 실증적 조사 또한 부족하다.



[그림 1] 연구 방향성 파이프라인

본 연구는 국내 클라우드 침해사고 대응 실무자 8명을 대상으로 설문을 수행하여, 침해사고 대응 6단계의 소요시간과 체감 난이도를 독립적으로 측정하고 환경 요인과 도구 요인을 분리하여 분석한다. [그림 1]은 본 연구의 전체 방향성을 나타내며, 현장의 실증적 고충 조사로부터 유동적 초동 대응 가이드라인의 필요성을

† 교신저자: 박기웅(세종대학교 정보보호학과 교수)

본 연구는 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.

도출하는 흐름을 보인다. 2장에서 설문 설계를, 3장에서 결과를, 4장에서 시사점과 향후 연구를 논의한다.

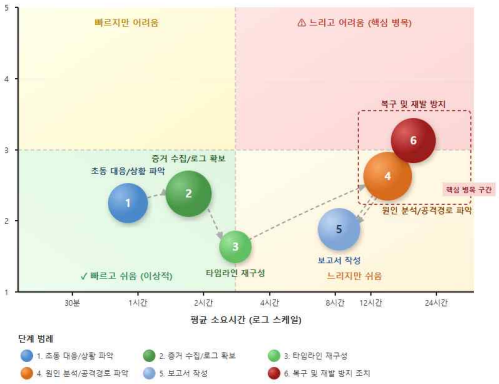
II. 설문 설계

본 설문은 클라우드 침해사고 대응 실무자의 고충을 시간적·인지적·환경적 세 차원에서 식별하기 위해 설계되었다. 문항은 응답자 특성(소속·직무·경력·주 대응 CSP), 대응 단계별 정량 측정, 환경 제약, 도구·자동화 요구, 정성 응답의 다섯 범주로 구성된다.

핵심 범주인 대응 단계별 측정에서는 침해사고 대응 프로세스를 (1) 초동 대응, (2) 증거 수집, (3) 타임라인 재구성, (4) 원인 분석, (5) 보고서 작성, (6) 복구 및 재발 방지의 6단계로 구분하고[4], 각 단계에 대해 소요시간과 체감 난이도(1~5)를 독립적으로 측정하였다. 두 지표를 분리한 이유는 "시간이 오래 걸리지만 쉬운 작업"과 "시간이 짧아도 판단이 어려운 작업"을 구별하여, 자동화가 필요한 지점이 물리적 지연인지 인지적 부담인지를 식별하기 위함이다.

환경 제약 범주에서는 로그 확보 시의 어려움(복수응답)과 "사고 현장에서 무엇부터 해야 할지 모른 경험"의 빈도를, 도구·자동화 범주에서는 현재 사용 도구와 자동화 희망 작업(최대 2개)을 수집하였다. 정성 응답으로는 가장 개선이 필요한 점을 자유 기술로 수집하여 정량 문항이 포착하지 못한 현장 맥락을 확보하였다. 설문은 2026년 4월 1일부터 7일까지 온라인으로 배포되었다.

III. 결과 분석



[그림 2] 침해사고 대응 단계별 시간x난이도

3.1 응답자 구성

총 8명의 유효 응답을 확보하였으며, 직군은 SOC 2명, 클라우드 보안 아키텍처 2명, CERT/CSIRT 1명, 침투테스트 1명, 제조업 보안 1명, 보안 운영 1명으로 분포한다. 경력은 1년 미만 2명, 1~5년 2명, 10년 이상 4명이며, 주 대응 환경은 AWS 6명, Azure 3명, GCP 2명, 국내 CSP(NCP·KT Cloud) 1명이다. 표본 규모는 제한적이나 직군·경력·환경의 다양성을 확보함으로써 탐색적 조사로서의 의의를 가진다.

3.2 단계별 시간·난이도 분석

[그림 2]는 6단계별 평균 소요시간(X축, 로그 스케일)과 체감 난이도(Y축)를 나타낸다. 분석 결과 복구 및 재발 방지(난이도 3.13)와 원인 분석(2.63) 두 단계에서 시간과 난이도가 동시에 가장 높게 나타났으며, 반면 타임라인 재구성(1.63)과 보고서 작성(1.88)은 상대적으로 낮았다. 이는 대응 부담이 단순 정리·보고가 아닌 인과 규명과 후속 조치 단계에 집중됨을 의미한다. 한 제조업 보안 담당자(10년+)는 "방대한 로그 속에서 최초 침입 경로(P0)를 찾는 게 제일 오래 걸리며, 못 찾으면 결과 보고서의 원인이 불분명해져 개선 대책이 나오지 않는다"고 서술하였는데, 이는 원인 분석의 실패가 후속 단계 품질까지 연쇄적으로 저하시킴을 보여준다.

3.3 로그 확보의 환경적 어려움

로그 확보 시 어려움으로는 로그 양 과다(5/8명), 어떤 로그를 봐야 하는지 모름(3명), 로그 보존기간 부족(3명), CSP별 로그 형식 상이(2명)가 지목되었다. 특히 "어떤 로그를 봐야 하

는지 모름"은 경력 3년 미만 응답자 3명에서 공통적으로 나타났으며, 이들은 "사고 현장에서 무엇부터 해야 할지 모른 경험"에 대해 모두 "자주 있다"고 응답하여 신규 대응자의 초동 단계 의사결정 부담이 일관된 패턴으로 관찰되었다.

3.4 자동화 요구사항

자동화 희망 작업으로는 ATT&CK[5] 매핑(5명), 타임라인 정리(4명), IOC 추출(3명), 로그 수집(3명)이 지목되었다. 흥미롭게도 실무자들이 가장 자동화를 원하는 작업은 3.2절에서 식별한 고난이도 작업(원인 분석·복구)과 일치하지 않는다. 이는 실무자들이 고난이도 작업 자체의 자동화보다 그 작업을 수행하기 위한 선행 정보 정리의 자동화를 우선시한다는 해석을 가능하게 한다. 즉, ATT&CK 기반 행위 매핑과 타임라인 재구성이 자동화될 때 분석가는 추론과 판단에 인지 자원을 집중할 수 있다.

IV. 논의 및 향후 연구

본 연구는 8명의 응답이라는 표본 한계를 지니며, 통계적 일반화보다는 클라우드 침해 대응 현장의 공통 병목을 식별하는 탐색적 조사로서의 의의를 가진다. 그럼에도 응답자의 직군·경력·대응 환경이 폭넓게 분포함으로써, 세 가지 발견 – (1) 인과 규명 단계의 병목, (2) 로그 환경의 파편성, (3) 선행 정보 정리의 자동화 요구 – 은 개별 직군에 국한되지 않는 공통 현상임을 시사한다.

주목할 점은, 응답자들이 공통적으로 지적한 어려움이 단일 도구나 정적 가이드라인으로 해소되기 어렵다는 것이다. 로그의 양·위치·보존 정책이 CSP와 조직마다 상이한 상황에서, 범용적 체크리스트는 현장 적용성이 떨어진다. 이는 사고 유형과 시스템 구성에 따라 동적으로 재구성되는 맞춤형 초동 대응 가이드라인, 그리고 이를 뒷받침하는 ATT&CK 기반 선행 정보 자동 정리 도구의 필요성을 제기한다.

향후 연구에서는 본 조사에서 도출된 요구사항을 바탕으로 (i) 국내 멀티 클라우드 환경(Naver Cloud, NHN Cloud, KT Cloud 등)에 특화된 지식베이스 설계, (ii) 사고 유형·시스템 구성 교차 매핑에 기반한 동적 가이드라인 생성 엔진, (iii) 오프라인 환경에서 동작하는 AI 보조 분석 파이프라인의 구체적 구현 및 현장 검증을 수행하고자 한다. 구체적으로, 유동적 가이드라인은 현장의 시스템 구성(CSP 종류, OS, 소프트웨어 스택)을 입력받아 해당 환경의 전체 데이터 흐름과 구성요소 간 연결 관계를 시각적으로 조망한 뒤, 사고 유형에 따라 수집 대상 아티팩트의 우선순위를 휘발성과 보존기한 기준으로 동적으로 제시하는 형태를 목표로 한다. 이를 통해 대응자는 개별 로그를 탐색하기 전에 시스템 전체의 구조를 파악하고, 어떤 지점에서 어떤 증거를 우선 확보해야 하는지를 직관적으로 판단할 수 있을 것으로 기대된다.

[참고문헌]

[1] 한국인터넷진흥원, 2024년 사이버위협 동향 보고서, KISA, December, 2024.

[2] 한국인터넷진흥원, 정보통신분야 침해사고 대응 안내서(개정본), KISA 보호나라 가이드라인, August, 2025.

[3] Cybersecurity and Infrastructure Security Agency, Federal Government Cybersecurity Incident and Vulnerability Response Playbooks, CISA, August, 2024.

[4] P.Cichonski, T.Millar, T.Grance and K.Scarfone, Computer Security Incident Handling Guide, NIST Special Publication 800-61 Revision 2, August, 2012.

[5] MITRE Corporation, ATT&CK Matrix for Enterprise: Cloud, MITRE ATT&CK Framework v15, April, 2024.