클라우드 포렌식 관점의 통합된 로그 분석 체계의 필요성

이지원*, 최상훈[1], 박기웅†

, [1] 세종대학교 SysCore Lab. (대학원생, 연구 교수[1])

†세종대학교 정보보호학과 (교수†)

The Necessity of an Integrated Log Analysis Framework for Cloud Forensics

Ji-Won Lee*, Sang-Hoon Choi[1], Ki-Woong Park†

, [1] Syscore Lab., Sejong University (Graduate Student, Research Professor[1])

†Dept. of Computer and Information Security, Sejong University

(Professor†)

요 약

클라우드 환경의 보안사고가 증가함에 따라 클라우드 포렌식의 중요성이 강조되고 있으며, 포렌식 분석에서는 로그의 역할이 핵심적이다. 그러나 현재 클라우드 로그는 서비스별로 구조가 상이하고 분산되어 있어 연계 분석과 행위 흐름 재구성에 한계를 가진다. 본 연구는 주요 클라우드별로 로그 수집을 비교하고 로그 분석을 통한 행위 재구성의 예시를 보여 포렌식 관점에서의 통합적 로그 분석 체계의 필요성을 제시한다. 나아가 통합적 로그 분석 체계의 구축을 위한 향후 연구 방향을 제시한다.

I. 연구 배경

클라우드 컴퓨팅 환경의 확산과 함께 클라우드 기반 서비스는 산업 전반에서 핵심 인프라로 자리 잡고 있다. 이에 따라 클라우드 환경을 대상으로 한 보안사고 또한 지속적으로 증가하고 있으며, 공격 기법 역시 점차 고도화되는 양상을 보여 클라우드 포렌식의 중요성이 강조되고 있다.

클라우드 포렌식 시 행위 흐름을 재구성하는 데에는 클라우드 로그가 중심적인 역할을 한다 [1]. 그러나 클라우드 환경은 단일 시스템 환경에 비해 공격 표면이 넓고 사고 발생 시 영향 범위 또한 광범위하다. 현재 클라우드는 서비스별로 상이한 로그 구조를 사용하고 있으며, 동일한 행위에 대해서도 서로 다른 형식으로 기록되는 경우가 많다. 단일 클라우드 내부에서도 서비스나 자원별로 다른 로그 구조를 사용하며, 중앙 집중적 수집이 이루어지지 않는 경우도 존재한다. 이러한 로그의 이질성과 파편화는 로그 간 연계 분석을 어렵게 만들어 사건 행위 흐름 재구성의 어려움으로 작용한다. 이에 본 연구에서는 포렌식 관점의 통합적인 로그 분석 체계의 필요성과 설계 방향성을 제시하여 보다 체계적인 클라우드 포렌식 환경 구축에 기여하고자 한다.

본 논문의 구성은 다음과 같다. 2장에서는 주요 클라우드 서비스 제공자들의 로그 수집을 비교하여 분석의 기반이 되는 통합된 구조의 필요성을 보인다. 3장에서는 단순한 공격 시나리오의 재구성 과정을 통해 로그의 연계 분석 과정을 보인다. 이를 통해 연계 분석에 유리한 포

† 교신저자: 박기웅 (세종대학교 정보보호학과 교수)
본 연구는 본 연구은 과학기술정보통신부의 재원으로 정보통신기획평가원 (IITP)의 정보보호핵심원천기술개발(Project No. RS-2026-25519773, 30%; RS-2024-004 38551, 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.

<표 1> 클라우드 서비스별 로그 수집과 통합 지원 여부 분석

CSP / Log	AWS [2]	Azure [3]	GCP [4]	Naver Cloud [5]	NHN Cloud [6]	KT Cloud [7]
Identity & Access	Cloudtrail (→ Cloudwatch)	Azure Monitor	Cloud Logging	Activity Tracer	CloudTrail	Log History
Resource & Control Plane	Cloudtrail (→ Cloudwatch)	Azure Monitor	Cloud Logging	Activity Tracer	Resource Watcher	Log History, Audit-User
Network	Flow Log (→ CloudTrail)	Network Watcher (→ Azure Monitor)	Cloud Logging	Flow Log (→ Cloud Log Analytics)	Flow Log	VPC Log
Storage Access	Cloudtrail (→ Cloudwatch)	Azure Monitor	Cloud Logging	Object Storage Log (→ Cloud Log Analytics)	CloudTrail	Object Storage Log
Database	RDS + Cloudwatch	Azure Monitor	Cloud Logging	DB Instance (→ Cloud Log Analytics)	DB Instance	DB Instance
Application	Agent (→ CloudWatch)	Agent (→ Azure Monitor)	Agent (→ Cloud Logging)	Agent (→ Cloud Log Analytics)	Log & Crash Search	KT Cloud Watch
Performance Metrics	Cloudwatch	Azure Monitor	Cloud Monitoring	Cloud Insight	Web service Monitoring System	KT Cloud Watch

렌식 관점의 객체 기준의 필요성을 보인다. 4장에서는 이러한 분석을 바탕으로 클라우드 포렌식 관점에서의 통합적 로그 분석 체계의 요구사항과 연구 방향을 제시한다.

II. 클라우드 서비스별 로그 수집 분석

클라우드 환경에서의 로그 수집 및 관리 방식은 CSP 및 서비스 유형에 따라 상이하게 구성되어 있으며, 이러한 차이는 포렌식 분석의 복잡성을 증가시키는 주요 요인으로 작용한다. 일반적으로 사용자 인증 및 행위 로그, 자원 생성 및 변경, 시스템 상태와 같은 로그는 대부분의 클라우드 환경에서 자동으로 수집된다. 그러나 다른 분류의 로그 수집에서는 서비스 제공자별 차이가 나타난다.

네트워크와 데이터베이스 로그의 경우, 이벤트나 감사 로그는 중앙 로깅 서비스에서 제공된다. 그러나 SQL 쿼리나 VPC Flow 로그와 같은 세부 행위 기록은 일부 CSP를 제외하면 각각의 DB와 VPC 내에서 수집되며 사용자의 설정을 통해 로그 시스템으로 전송되어야 한다. 이러한 구조는 행위 분석 시 로그의 누락 가능성을 증가시키며, 전체 트래픽 흐름을 일관되게 파악하는 데 어려움을 초래한다. 스토리지 접근 로그 역시 일부 CSP를 제외하고는 해당 스토리지에서 수집되어 중앙으로 전송하도록 설정해 주어야 하는 경우가 대부분이다.

애플리케이션 로그는 에이전트 설치를 통해 중앙 로그 수집 서비스로 전송되며, 서비스 특성상 가장 분산되어 있으나 대부분 중앙으로의 수집을 지원한다. 그러나 이는 사용자의 설정에 대한 의존도가 높다.

종합적으로 볼 때, 현재 대부분의 클라우드 로그의 수집 범위와 위치가 분산되어 있다. 해외 CSP들이 국내에 비해 로그 서비스로의 수집이 용이하도록 지원하는 범위가 비교적 넓으나 여전히 대부분의 CSP에서 세부 로그는 사용자의 설정을 거쳐 수집하는 과정이 필요하다. 또한 수집된 로그 형식이 서로 이질적이며 로그 간의 통합도 제한적이다.

따라서 클라우드 포렌식 관점에서 로그의 유의미한 상관관계를 분석하기 위해서는 파편화되

고 이질적인 로그 데이터를 한 곳에 수집하여 통일된 구조로 재구성할 필요가 있다.

III. 클라우드 로그 기반 행위 재구성 과정 분석

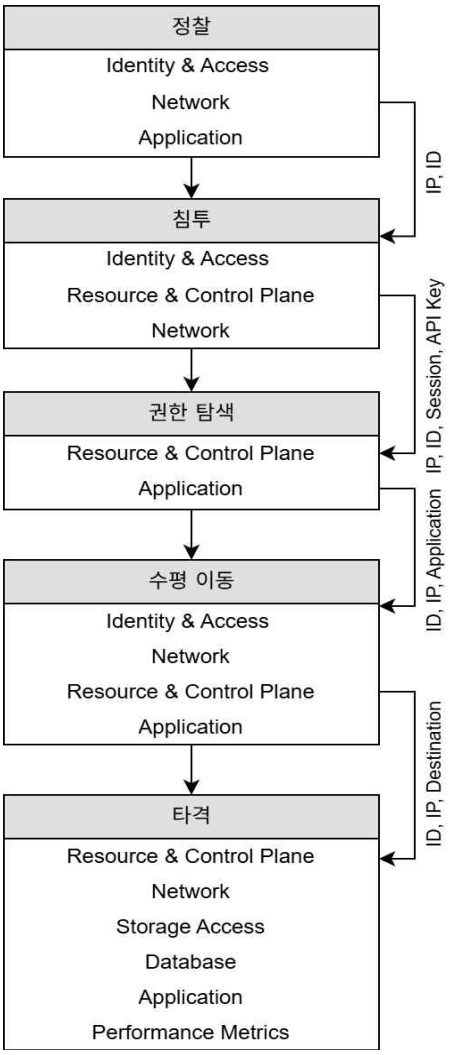

그림 1. 공격 단계별 관련 로그 연계

해당 표는 5단계로 구성된 간단한 공격 시나리오를 가정하여, 클라우드 환경에서 발생하는 공격 행위를 로그 간의 연계를 통해 추적하는 과정을 나타낸다. 공격의 각 단계는 ID와 같은 식별자를 통해 직접적으로 연결될 수도 있지만, 동일한 세션이나 IP와 같은 논리적 위치를 기반으로 연결되기도 한다. 또한 트래픽의 송수신 지점이나 행위의 대상과 같은 관계를 통해서도 로그 간 연계 분석이 가능함을 확인할 수 있다.

이를 통해 클라우드 환경에서의 공격 행위는 단일 로그가 아닌 다양한 계층의 로그에 분산되어 나타난다는 점을 확인할 수 있다. 특히 하나의 공격 단계에서도 Identity, Network, Resource, Application, Storage 등 서로 다른 관점의 로그가 동시에 필요하다는 사실은 개별 행위를 단일 로그만으로는 충분히 설명할 수 없음을 시사하여 로그의 통합적 분석이 필요함을 알 수 있다.

또한 각 로그를 연결하는 항목들을 통해, 단편적인 사건들의 기록을 하나의 행위 흐름으로 연결하는 요소가 무엇인지 파악할 수 있다. 이러한 연결 항목들은 단순한 필드 값이 아니라, 실제 행위를 구성하는 의미 있는 요소로 해석될 수 있다. 예를 들어 UserID나 API Key는 행위자를 나타내고, IP나 Session은 행위가 발생한 위치를 의미하며, Destination이나 Application은 행위의 대상 자원을 지칭한다. 또한 API 호출이나 프로세스 정보는 수행된 동작을 나타내고, 네트워크 트래픽이나 데이터 변경 기록 등은 행위의 결과로 해석될 수 있다.

이처럼 로그 간 연결에 사용되는 필드들은 행위의 구성 요소로 귀결된다. 그러나 이러한 요소들은 각각 서로 다른 로그와 필드에 분산되어 존재하기 때문에, 단순히 로그를 나열하거나 필드 단위로 매칭하는 방식만으로는 전체 행위 흐름을 온전히 재구성하기 어렵다.

따라서 공격 행위를 정확하게 재구성하기 위해서는 분석의 기준을 행위 구성 요소를 중심으로 전환할 필요가 있다. 즉, 서로 다른 로그에 분산된 데이터를 행위자, 위치, 자원, 동작, 결과와 같은 공통된 기준으로 재구성하고, 이를 하나의 맥락으로 통합하는 접근이 요구된다.

이와 같은 관점에서 포렌식 중심의 객체 기반 로그 분석의 필요성이 드러난다. 객체 기반 분석은 식별자를 중심으로 로그를 묶는 것을 넘어, 이들이 동일한 행위자, 동일한 자원, 동일한 데이터 객체를 가리킨다는 점을 전제로 관계를 재구성하는 것이다. 이를 통해 분산된 로그를 하나의 행위 흐름으로 통합할 수 있으며, 공격의 전체 경로를 일관된 맥락에서 이해할 수 있게 될 것이다. 이러한 객체 기반 접근은 단계 기반 분석이 갖는 한계를 보완하며, 복잡한 클라우드 환경에서 실제 공격 흐름을 효과적으로 재구성하기 위해 필수적이다.

IV. 결론 및 향후 연구

본 연구에서는 클라우드 포렌식을 위한 통합된 로그 분석 체계의 필요성을 제시하였다. 클라우드 포렌식의 중요도가 증가하는 가운데 클라우드 로그는 여전히 상이한 로그 구조와 분산된 수집 방식으로 인해 로그 간 연계 분석이 어려우며, 이러한 한계는 클라우드 포렌식의 정확성과 효율성을 저해한다.

클라우드별 로그 수집 분석을 통해 클라우드 로그가 파편화되어 있으며, 수집 범위와 형식이 일관되지 않아 통합적 수집 및 구조 통합이 필요함을 확인하였다. 또한 공격 시나리오 가정을 통해 행위 관련 로그와 연계 분석을 위한 필드를 분석함으로써 단순한 구조 통합이 아닌 행위 객체 기반의 분석 체계에 대한 필요를 확인할 수 있었다.

향후 연구에서는 먼저 클라우드 환경에서 생성되는 이질적인 로그 데이터를 통합적으로 활용하기 위해, 서로 다른 형식과 구조를 갖는 로그를 일관된 형태로 정규화하는 데이터 구조 통합이 선행될 필요가 있다. 이를 위해 CSP별로 상이한 로그 포맷을 공통 스키마로 변환하고, JSON 기반의 구조로 정의하여 다양한 로그를 통합된 형태로 표현할 수 있는 체계를 설계해야 한다.

이와 함께, 단순한 구조 통합을 넘어 로그를 행위 구성 요소 단위로 해석하고 재구성할 수 있도록 객체 기반 표현 모델을 정의할 필요가 있다. 즉, 행위자, 자원, 데이터, 네트워크 위치 등과 같은 객체를 중심으로 로그를 재구성하고, 서로 다른 로그에 분산된 필드들이 동일한 객체를 지칭할 수 있도록 관계를 정의함으로써, 행위 흐름을 일관된 맥락에서 파악할 수 있는 데이터 모델을 구축해야 한다.

마지막으로, 이러한 통합 구조와 객체 기반 모델을 바탕으로 실제 포렌식 분석을 수행할 수 있는 분석 프로그램의 개발이 요구된다. 이는 CSP별 로그를 자동으로 수집, 파싱 및 변환하는 기능을 포함할 뿐만 아니라, 객체 간 관계를 기반으로 사건 흐름을 시각화하고 연관 이벤트를 분석할 수 있는 기능을 제공해야 한다. 이를 통해 분산된 로그 데이터를 유기적으로 연결하고, 복잡한 공격 행위를 보다 직관적으로 재구성할 수 있을 것으로 기대된다. 나아가 이러한 체계는 분석 과정에서 도출된 패턴과 관계를 축적하여 보안 인텔리전스로 발전시킬 수 있으며, 궁극적으로 클라우드 환경 전반의 보안 수준 향상에 기여할 수 있을 것이다.

[참고문헌]

[1] S. Khan, A. Gani, A. W. A. Wahab, M. A. Bagiwa, M. Shiraz, S. U. Khan, R. Buyya and A. Y. Zomaya, Cloud Log Forensics: Foundations, State of the Art, and Future Directions, ACM Computing Surveys, vol. 49, no. 1, Article 7, May, 2016.

[2] Amazon Web Services, AWS CloudTrail User Guide, Available: https://docs.aws.amazon.com/awscloudtrail/, Accessed: April, 2026.

[3] Microsoft, Azure Monitor Documentation, Available: https://learn.microsoft.com/en-us/azure/azure-monitor/, Accessed: April, 2026.

[4] Google Cloud, Cloud Logging Overview, Available: https://cloud.google.com/logging/docs, Accessed: April, 2026.

[5] NAVER Cloud, NAVER Cloud Platform User Guide, Available: https://guide.ncloud-docs.com/docs/home, Accessed: April, 2026.

[6] NHN Cloud, NHN Cloud User Guide, Available: https://docs.nhncloud.com/ko/nhncloud/ko/user-guide/, Accessed: April, 2026.

[7] KT Cloud, KT Cloud Education Basic Guide, KT Cloud Manual, Release Date: October 8, 2024, Available: https://manual.cloud.kt.com/kt/education-edubasic-edu_ess_1, Accessed: April, 2026.