JDCS
디지털콘텐츠학회논문지
Journal of Digital Contents Society
Vol. 27, No. 4, pp. 1159-1167, Apr. 2026

Check for updates

클라우드 컴퓨팅 서비스 보안사고 대응을 위한 포렌식 분석 프레임워크

서 승 희*
한국전자통신연구원 부설연구소 연구원

A Forensic Analysis Framework for Security Incident Response in Cloud Computing Services

Seunghee Seo*
Researcher, The Affiliated Institute of ETRI, Daejeon 34186, Korea

[요 약]

클라우드 컴퓨팅 서비스의 활발한 정부·공공기관과 민간기업에서의 도입에 따라 이를 대상으로 한 계정 탈취, 데이터 유출, 서비스 마비, 자원 도용 등의 보안사고 발생 빈도가 급격히 증가했다. 이에 따라, 클라우드 컴퓨팅 서비스 도입 환경에서 보안사고 발생 시 피해확산 및 사고 재발 방지, 행위자 추적 및 법적 처벌을 위한 적절한 보안사고 조사 절차와 방안이 필요하다. 하지만 기존 클라우드 보안사고 포렌식 절차는 클라우드 서비스 제공 업체(CSP)의 협조를 전제하거나 서버 인프라 측면의 조사를 배제하고 있어 실제적인 적용이 어렵다. 따라서, 본 논문에서는 CSP에서 제공하는 테넌트의 인프라 자원 이용에 관한 기록을 기반으로 실질적인 인프라 측면의 조사 절차를 포함한 클라우드 보안사고 포렌식 프레임워크를 제안한다. 본 논문에서는 데이터 주체와 서비스 관점에서 조사 대상을 정의하고 클라우드 서비스 유형에 따른 분류를 기반으로 클라우드 보안사고 포렌식 프레임워크를 5단계로 구성하였다. 또한, 네이버 클라우드를 분석하고 제안하는 프레임워크의 적용방안을 확인하였다.

[Abstract]

The rapid adoption of cloud computing services across government, public institutions, and private enterprises has led to a sharp increase in security incidents, such as account hijacking, data breaches, service disruption, and resource abuse. Accordingly, there is a growing need for effective forensic procedures to prevent damage escalation and recurrence, as well as to enable attacker attribution and legal accountability in cloud environments. However, existing cloud forensic approaches often assume cooperation from cloud service providers (CSPs) or exclude infrastructure-level investigations, limiting their practical applicability. This study proposes a cloud security incident forensic framework that incorporates infrastructure-level investigation procedures based on tenant resource usage records provided by CSPs. The framework defines investigation targets from both data-centric and service-centric perspectives. It consists of five stages, structured according to cloud service models. To validate the applicability of the proposed framework, a case study using Naver Cloud was conducted.

색인어 : 클라우드 포렌식, 클라우드 사고대응, 클라우드 컴퓨팅, 클라우드, 디지털 포렌식
Keyword : Cloud Forensics, Cloud Incident Response, Cloud Computing, Cloud, Digital Forensics

http://dx.doi.org/10.9728/dcs.2026.27.4.1159

Received 26 March 2026; **Revised** 06 April 2026
Accepted 15 April 2026

***Corresponding Author; Seunghee Seo**
Tel: ※ 개인정보 표시제한
E-mail: sh.seo.713@gmail.com

Ⅰ. 서 론

클라우드 컴퓨팅 서비스는 개발 환경, 연산 및 저장 자원, 서비스 인프라 등을 인터넷을 기반으로 제공하는 서비스로, 인프라를 구축하고 유지보수하는 비용을 절약할 수 있고 각종 자원 증·감축이 편리하다는 장점이 있다. 또한, 대규모 연산 자원을 지원하는 대형 클라우드 서비스 공급업체가 늘어남에 따라 연산 자원이 크게 요구되는 인공지능, 빅데이터, 블록체인 기반 서비스 구축에 많이 활용되고 있다. 이에 따라 최근 정부에서는 신속·유연성 제공, 운영비 절감 등을 목표로 행정·공공기관의 정부 서비스를 클라우드로 전환하는 '공공 클라우드 전환사업'을 시행하고 있다[1].

하지만 공공기관과 민간기업의 클라우드 컴퓨팅 서비스에 대한 의존도가 높아짐에 따라 계정 탈취, 데이터 유출, 서비스 마비, 자원 도용(불법 암호화폐 채굴) 등의 보안사고 발생 빈도가 급격히 증가하고 있다. 보안 업체인 체크포인트의 Cyber Security Report 2023[2]에 따르면, 클라우드 서비스에 대한 사이버 위협은 지난 1년간 48% 증가하였다. 이에 따라 국내에서는 최근 안전한 클라우드 컴퓨팅 서비스 도입 환경 구성을 위한 법률[3]과 보안 인증제도[4],[5]를 시행하고 있다. 하지만 클라우드 컴퓨팅 서비스 도입 환경에서 사이버위협 예방을 위한 보안 강화도 중요하지만, 보안사고 발생 시 피해확산과 사고 재발을 방지하기 위해서는 보안사고 조사 및 대응을 위한 적절한 절차와 방안이 필요하다[6].

보안사고에 대한 포렌식 조사 시, 클라우드 컴퓨팅 서비스 도입 환경은 서버 인프라를 자체적으로 구축하고 보유하는 기존 온프레미스 환경과 달리 인프라와 서버 구동 환경에 관한 데이터 통제권이 이용자가 아닌 클라우드 컴퓨팅 서비스 제공 업체가 갖는다. 이에 따라, 클라우드 컴퓨팅 인프라를 구성하는 하드웨어에 접근을 통한 물리적인 데이터 획득은 클라우드 컴퓨팅 서비스 공급자(Cloud Service Provider, CSP)의 개입이 필요하다. 하지만 클라우드 컴퓨팅 서비스 공급자(이하 CSP)의 협조를 기대하기 어렵고[7], CSP가 협조하더라도 다중 국가에 서버 인프라가 분산된 대규모의 국외 클라우드 컴퓨팅 서비스의 경우 보안사고와 관련한 데이터가 국외에 위치한다면 물리적인 데이터 획득은 사건의 유형에 따라 해당 국가의 협조가 요구될 수 있다는 제약이 있다. 하지만 기존 클라우드 보안사고 포렌식 절차는 CSP가 협조한다는 가정하에 인프라의 물리적 데이터 수집과 조사를 고려[8]-[11]하거나 인프라 측면의 조사를 배제[12]하고 있어 사고 발생 시 실제적인 적용이 어렵다. 일부 연구에서는 테넌트의 활동 기록을 반영[13]하였으나, 테넌트의 궁극적인 목적의 서비스를 이용하는 최종 사용자에 관한 조사나 실제적인 적용에 관한 분석이 포함되어야 한다.

따라서, 본 논문에서는 CSP의 협조를 기대하기 어렵더라도, CSP가 사용자에게 제공하는 인스턴스 생성·접근·사용 로그, 리소스 관련 API·SDK 사용 로그 등 인프라 자원의 이용에 관한 이벤트 기록을 기반으로 인프라 측면을 포함한 클라우드 컴퓨팅 서비스 보안사고 포렌식 프레임워크를 제안한다. 클라우드 컴퓨팅 서비스는 물리적인 인프라 자원을 인터넷 계정에 따라 논리적으로 구분하고 가상화하여 서비스한다. 일부 CSP는 사용자가 서비스 관리와 보안 모니터링을 수행할 수 있도록 사용자의 계정이 관여하는 논리적인 영역에 한정하여 클라우드 컴퓨팅 인프라 이벤트 기록을 제공하고 있다. 이는 보안사고 발생 시, 사고 발생 원인과 경위를 파악하고 책임 소지의 판단이나 악의적으로 사고를 일으킨 가해자를 추적할 때 정황 증거나 직접 증거를 수집하는 단서로 활용될 수 있다.

본 논문에서는 클라우드 컴퓨팅 서비스의 데이터 주체와 서비스 관점에서 보안사고 발생 시 조사 대상을 정의하고 Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS), Desktop as a Service (DaaS)의 클라우드 서비스 유형에 따른 조사 대상을 분류한다. 그리고 이를 기반으로 클라우드 서비스 유형 및 조사대상 범주 식별, 조사 대상의 데이터 접근 권한 식별 및 필요 권한 요청, 조사 대상별 관련 데이터 수집, 수집 데이터 분석, 사고 보완 조치 및 재발 방지 대응의 5단계로 구성된 클라우드 컴퓨팅 보안사고를 조사하는 프레임워크를 제안한다. 또한, 제안하는 프레임워크의 실제적인 적용 가능 방안을 확인하기 위해 국내 상용 클라우드인 네이버 클라우드에서 웹 서비스 환경을 구성하고 포렌식 조사를 위해 필요한 인증 정보 및 권한 확인, 서비스 가용에 따른 데이터 수집 및 분석을 수행할 결과를 제시한다.

본 논문에서 제안하는 프레임워크는 실제 조사 상황을 반영하여 Cloud Service Provider(CSP)의 협조 요청 필요성과 협조 여부를 고려하고 이에 따른 조사 절차를 구분함에 따라, 기존 클라우드 컴퓨팅 포렌식 프레임워크에 관한 연구와 차별성을 갖는다. 그리고 클라우드 컴퓨팅 서비스를 도입하여 제공하는 실제 서비스에 중점을 두고, 조사 대상 구분과 클라우드 서비스 유형의 특성을 고려한 조사 대상 범주를 설정함에 따라 클라우드 컴퓨팅 서비스 자체만을 범주로 하는 기존 연구보다 확대된 프레임워크를 제시한다.

본 논문은 2장에서 보안사고 조사 대상 유형을 정의하고 클라우드 컴퓨팅 서비스 유형별 조사 대상을 분석한다. 3장에서 제안하는 클라우드 컴퓨팅 서비스 보안사고 포렌식 프레임워크에 대해 설명하고, 4장에서 Naver Cloud의 Cloud Activity Tracer 분석을 통해 제안하는 클라우드 컴퓨팅 서비스 보안사고 포렌식 절차의 적용 가능성을 확인한다. 그리고 5장에서 결론으로 마무리한다.

Ⅱ. 클라우드 컴퓨팅 서비스 유형별 조사 대상 분석

국가·공공기관과 민간기업에서 클라우드 컴퓨팅 서비스는 해당 기관에서 특정 서비스(기능)를 고객이나 내부 직원에게 제공하기 위해 활용하기 위해 도입될 수 있다. 즉, 특정 서비

스 구축을 클라우드 컴퓨팅 서비스의 인프라를 이용하는 것으로 국가·공공기관과 민간기업은 클라우드 컴퓨팅 서비스 이용자이면서 특정 서비스를 공급하는 공급자이다. 그리고 클라우드 컴퓨팅 서비스의 인프라를 기반으로 하는 궁극적인 서비스의 최종 이용자는 국민, 고객, 내부 직원이다. 이에 따라, 본 논문에서는 보안사고 발생 시, 관련 데이터의 주체와 서비스의 제공·이용 관점에 따라 그림 1과 같이 조사 대상 유형을 클라우드 서비스 공급자 (CSP), 클라우드 서비스 이용자 (CSU), 최종 사용자 (EU)로 정의한다. 그림 1의 각 조사 대상 유형에 대한 설명은 다음과 같다.

- Cloud Service Provider (CSP): 클라우드 컴퓨팅 플랫폼을 구축하여 인프라, 애플리케이션 및 스토리지, 데스크톱, 개발 환경 등의 서비스를 제공하는 자(또는 업체). 클라우드 서비스 인프라 자체에 관련한 데이터의 권한 및 통제권 소유
- Cloud Service User (CSU): 호스팅한 클라우드 컴퓨팅 자원을 기반으로 특정 목적의 서비스를 구축하고 최종 이용자에게 궁극적인 최종서비스를 제공하는 자(테넌트). 특정 목적의 서비스 구동에 관한 데이터 권한 및 통제권 소유
- End User (EU): 클라우드 컴퓨팅 인프라를 기반으로 제공되는 특정 목적의 서비스를 직접 사용하는 최종 이용자. 특정 목적의 서비스에 기반이 되는 데이터(리소스)의 권한과 통제권 소유

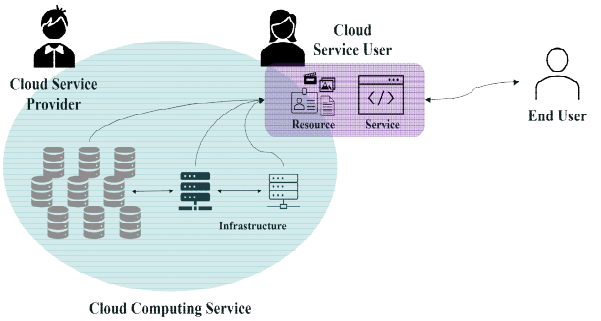


그림 1. 클라우드 컴퓨팅 서비스 사고조사 대상 유형
Fig. 1. Types of investigation targets for cloud computing service incident investigation

클라우드 컴퓨팅은 지원하는 서비스의 형태에 따라 Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS), Desktop as a Service (DaaS)의 4가지 유형으로 분류할 수 있다 [14]. 각 클라우드 서비스 유형은 플랫폼의 지원 범위와 목적이 각각 다르므로 포함하는 조사 대상의 범위와 각 조사 대상에 수집해야 하는 데이터의 종류가 다르다. 본 논문에서 클라우드 컴퓨팅 서비스 유형에 따른 특성과 이를 기반으로 지정한 조사 대상 범위는 표 1과 같다.

표 1에서 IaaS는 이용자가 가용할 수 있는 서비스 범주가 가장 큰 유형으로 모든 조사 대상 유형을 포함한다. 반면, SaaS, DaaS는 CSP가 모든 자원과 서비스 인프라를 구축하고 제공하는 서비스 자체가 곧 궁극적인 서비스이므로 조사

표 1. 클라우드 컴퓨팅 서비스 유형별 조사 대상 범주 및 설명
Table 1. The categories and descriptions of investigation targets by cloud computing service type

Cloud computing service type	Description	Investigation targets by service type		
		Cloud service provider (CSP)	Cloud service user (CSU)	End user (EU)
Infrastructure as a Service (IaaS)	• Provides virtualized infrastructure resources, such as servers, storage, and networks, for building specific services • Includes end users, cloud service users, and cloud service providers	✓	✓	✓
Platform as a Service (PaaS)	• Provides a virtual environment for using platform resources for service development without separate infrastructure deployment • Since the application/service itself may use the user's own infrastructure or other cloud services, end users exist outside the cloud service	✓	✓	
Software as a Service (SaaS)	• Provides application software services over the network without requiring separate environment configuration or installation • The cloud service provider controls both services and resources, so the cloud service user is effectively the cloud service provider	✓		✓
Desktop as a Service (DaaS)	• Provides virtualized desktops and installed application software services over the network • The cloud service provider controls all services and resources and delivers the final service requested by the end user	✓		✓

대상으로는 EU와 CSP만 포함한다. PaaS의 경우, 궁극적인 서비스를 개발할 수 있는 플랫폼을 제공하는 유형으로 개발한 서비스(제품)을 구동하는 환경은 클라우드 환경이 아닐 수 있다. 이에 따라, 최종 이용자(EU)는 조사 대상 범주에서 제외한다.

Ⅲ. 클라우드 컴퓨팅 서비스 보안사고 포렌식 절차

본 장에서는 2장에서 정의한 조사 대상과 클라우드 컴퓨팅 서비스 유형에 따른 조사 대상 범위를 기반으로 클라우드 컴퓨팅 보안사고 포렌식 프레임워크를 제안한다. 본 논문에서 제안하는 (1) 클라우드 서비스 유형 및 조사 대상 범주 식별, (2) 조사 대상의 데이터 접근 권한 식별 및 필요 권한 요청, (3) 조사 대상별 관련 데이터 수집, (4) 수집 데이터 분석, (5) 사고 보완 조치 및 재발 방지 대응의 5단계로 구성된 클라우드 컴퓨팅 보안사고 포렌식 프레임워크는 그림 2와 같다. 그리고 그림 2의 각 단계에 대한 설명은 다음과 같다.

3-1 클라우드 서비스 유형 및 조사 대상 범주 식별

그림 2의 (1)과 같이 클라우드 서비스 유형 및 조사 대상 범주 식별 단계에서는 먼저 조사해야 하는 클라우드 컴퓨팅 서비스의 유형이 앞서 설명한 IaaS, PaaS, SaaS, DaaS 중 어디에 해당하는 지 판별한다. 조사 대상 환경의 서비스 유형이 판별되면, 해당 서비스 유형의 조사대상 범주에서 사건 유형의 특성을 고려하여 조사대상의 포함 여부를 판별한다. 또한, 이 단계에서는 클라우드 서비스의 유형과 포함해야 하는 조사 대상을 식별할 뿐 아니라 전체적인 보안사고 조사 전략을 수립하여 가장 중요한 단계인 데이터 수집과 분석 과정을 체계적으로 수행하도록 해야 한다.

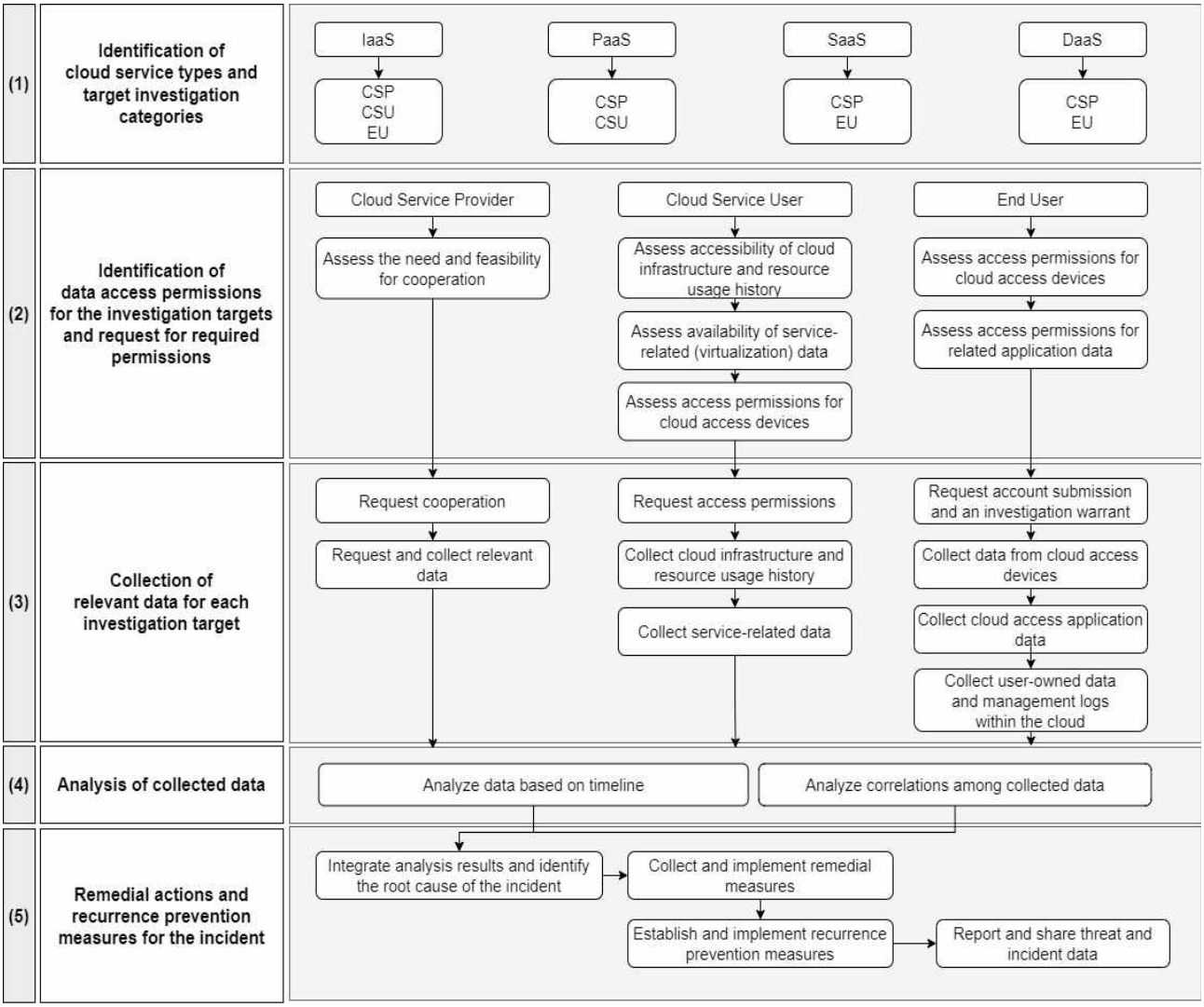


그림 2. 제안하는 클라우드 컴퓨팅 서비스 보안사고 포렌식 프레임워크

Fig. 2. Proposed forensic framework for cloud computing service security incidents

3-2 조사 대상의 데이터 접근 권한 식별 및 필요 권한 요청

그림 2의 (1)단계에서 조사 대상이 확정되면 각 대상이 제공할 수 있는 데이터나 서비스의 범주를 파악하고, 관련한 데이터를 수집하기 위해 필요한 협조나 권한, 계정, 기타 제약사항 등을 확인한다. 필요한 권한 및 계정이 식별되면 확보하기 위한 제출 요청, 압수 영장 발부, 협조 요청 등의 절차를 수행한다.

CSP의 경우, 먼저 CSU나 EU에서 클라우드 컴퓨팅 서비스 인프라에 관한 데이터 수집 범주를 파악하고, 해당 수집 범주 내에서 보안사고 조사가 어렵다고 판단된 경우에 협조를 요청한다. 예를 들어, 고의적인 테넌트 로그 삭제로 클라우드 인프라 측면의 저수준 로그나 물리적 데이터 접근이 필요한 경우나, 클라우드 인프라의 보안 결함에 따른 침입이 의심되는 경우 CSP의 협조가 필요하다고 판단할 수 있다. 하지만 클라우드 컴퓨팅 서비스 자체적으로 메모리, 네트워크, 디스크 등의 인프라 리소스 사용에 관한 로그를 제공하며 보안사고 범위가 테넌트 외 인프라 범주에 미치지 않으면 CSP의 협조는 필수적이지 않다.

CSU에 대해서는 클라우드 컴퓨팅 인프라 관련 데이터 접근 권한과 구축한 서비스와 관련한 데이터 접근 권한을 확인하고 관련 권한을 소유한 별도의 계정을 요청하거나 관리자나 매니저 계정을 확보해야 한다.

EU는 CSU가 제공하는 서비스를 이용하는데 사용한 단말 디바이스에 대한 조사가 필요하다. 서비스 이용 형태(애플리케이션, 웹 등)와 이에 사용한 단말 디바이스의 종류(모바일, 데스크톱 등)를 식별해야 하고 해당 디바이스 내부에 기록된 서비스 이용 기록 수집에 필요한 계정이나 디바이스 패스워드 등의 필요 여부를 판별해야 한다. 그리고 이를 확보하기 위해 제출을 요청하거나, 사건의 유형에 따라 강제해야 할 시 압수 영장 발부 등의 절차가 필요할 수 있다.

3-3 조사 대상별 관련 데이터 수집

앞선 그림 2의 (2)단계에서 각 조사 대상에 대해 데이터 수집에 필요한 권한, 계정, 디바이스 등이 확보되면 발생한 보안사고와 관련한 데이터를 수집한다. 보안 사고 발생 경위와 원인 파악을 위해서는 이전 시스템의 변화를 추적하는 것이 중요하다. 이에 따라, 클라우드 컴퓨팅 서비스 자원이나 인프라 사용에 관한 로그 데이터 수집이 반드시 필요하다.

클라우드 컴퓨팅 서비스는 CSP의 협조에 따른 물리적 데이터 수집이 아니면, EU의 디바이스를 제외한 모든 데이터 수집 과정은 인터넷을 통해 이루어진다. 인터넷을 통한 수집은 물리적 복제와 달리 구동 중인 서비스 접근이 불가피하므로, 수집 과정에서 시스템 로그 등의 사건 조사에 필요한 주요 파일의 내용이 변조되거나 삭제되지 않도록 유의해야 한다. 특히, 파일을 단순 복사할 경우 메타데이터가 시스템 내 원본과 달라지므로 메타데이터를 포함한 덤프를 수행해야 한다. 그리고 수집한 원본 파일은 별도의 저장 장치에 해시값과 함께 관리하고 분석 시 복제하여 사용한다.

클라우드 컴퓨팅 서비스 자원이나 인프라 사용에 관한 데이터를 제외하고 가상머신(인스턴스) 내 데이터 수집 절차는 일반적인 컴퓨팅 포렌식 절차와 유사하게 수행할 수 있다. 다만, IaaS, PaaS의 경우, CSU가 구축한 서비스의 종류와 로깅, 데이터 관리 방식에 따라서 데이터 수집 절차가 상이할 수 있다. 클라우드 컴퓨팅 서비스 유형별 조사 대상에 따른 수집 데이터의 종류 예시는 표 2와 같다.

3-4 수집 데이터 분석

수집 데이터 분석 단계는 각기 다른 조사 대상에서 수집한 데이터들을 분류하거나 재배열하고, 데이터들의 순서와 연관성, 해당 관계들의 의미를 분석함으로써 보안사고 발생 경위와 원인을 파악하는 단계이다. 단일 데이터는 자체적으로 사실관계나 행위를 의미할 수도 있지만, 시간 순서에 따른 데이터 간의 연결이나 의미론적 측면에서의 관계 분석은 새로운 사실관계나 행위, 의도 등을 추론하고 증명하는데 활용될 수 있다.

본 논문에서는 수집 데이터 분석 단계를 그림 2의 (4)와 같이 크게 타임라인에 따른 데이터 분석과 수집 데이터 간 연관성 분석로 나누었다. 타임라인에 따른 데이터 분석 절차에서는 수집한 데이터들을 시간 순서에 따라 정리하고 일정 시간 단위별로 나타나는 일관성 있는 데이터 집합이나 패턴을 분석함으로써 시간에 따른 시스템이나 사용자의 행위와 순서를 파악할 수 있다. 수집 데이터 간 연관성 분석 절차에서는 각기 다른 조사 대상에서 수집된 데이터들을 종합하여 서로 갖는 관계성을 분석을 통해 사용자 또는 공격자의 의도나 단순한 데이터 정렬로 확인하기 어려운 행위를 추정한다.

3-5 사고 보완 조치 및 재발 방지 대응

그림 2의 (5)의 사고 보안 조치 및 재발 방지 대응 단계에서는 각 기준에 따른 수집 데이터 분석 결과를 종합하여 보안사고 발생원인과 발생 경위를 규명한다. 그리고 보안사고의 피해확산을 방지하기 위해 발생 원인이 되는 취약성을 보완하고, 동일한 사고가 반복되거나 유사한 방식으로 다른 보안사고가 발생하지 않도록 사고 재발 방지 대책을 수립하고 이행해야 한다. 예를 들어, 부주의한 관리로 인한 CSU의 관리자 계정 정보 유출이 보안사고 발생의 원인일 경우, 관리 계정 정보 변경을 통해 침입 경로를 차단함으로써 피해확산을 방지하고 관리자 계정 정보 관리 방식을 안전하게 변경함으로써 이를 이용한 보안사고의 재발생을 예방할 수 있다.

모든 보완조치가 이행되고 나면 보안사고에 관한 보고서를 작성하고 기관이나 기업의 보고 체계에 따라 조사 내용을 보고하거나 법집행기관 또는 법정에 제출한다. 만약, 해당 사고가 다른 클라우드 컴퓨팅 서비스 도입 환경의 서비스에도 위협이 될 것으로 판단되면 사이버 위협 인텔리전스(CTI) 등의

표 2. 클라우드 컴퓨팅 서비스 유형별 조사 대상에 따른 수집 데이터 종류
Table 2. Types of collected data based on investigation targets by cloud computing service type

Investigation target types	IaaS (infrastructure as a service)	PaaS (platform as a service)	SaaS (software as a service)	DaaS (desktop as a service)
Cloud Service Provider (CSP)	– Physical system logs – Service user management history – Service users' resource usage history (requested resource type and quantity, request time, usage duration, etc.) – Information on resource location and data transfer paths of service users	– Physical system logs – Service user management history – Service users' resource usage history (resource request time and usage duration) – Project storage location and transfer history of service users – Project creation, modification, and deletion history	– Physical system logs – User management history – Storage location and transfer history of user resources – Resource storage, modification, and deletion history – Resource request and response history	– Physical system logs – User management history – User resource usage history – Storage location and transfer history of user resources – Resource storage, modification, and deletion history – Resource request and response history
Cloud Service User (CSU)	– Administrator account access and usage history – User account management history – Service request and response history – Data access permission management history – OS and system operation logs – Cloud infrastructure resource usage logs (Storage, Network, Instance, etc.)	– Account creation and deletion history – Account access and usage history – Development information and code creation/deletion history – Development information and code modification/sharing history – Development group creation and sharing history – Project creation history – Project deployment history		
End User (EU)	– Account creation and deletion history – Account access and usage history – Personal data access history – Personal data storage history – Service usage history		– Account creation and deletion history – Account access and usage history – Personal data access history – Personal data storage history – Service and function usage history	– Account creation and deletion history – Account access and usage history – Virtual machine (desktop) creation and deletion history – OS installation and internal operation logs

공유 시스템을 활용하여 관련 기관에 보안사고 정보를 공유하는 것이 좋다.

Ⅳ. 네이버 클라우드에 대한 포렌식 분석

본 장에서는 국내 상용 클라우드인 네이버 클라우드에서 웹 서비스를 구축하고, 제안하는 클라우드 보안사고 포렌식 프레임워크를 기반으로 포렌식 분석을 수행한 결과를 설명한다. 본 논문에서 분석을 위해 구성한 실험 환경은 그림 3과 같다.

4-1 조사 대상의 데이터 접근 권한 식별 및 필요 권한 요청 단계

그림 3의 네이버 클라우드 기반 웹 서비스는 클라우드 서비스 유형이 IaaS이고 조사 대상으로 CSP, CSU, EU를 모두 포함한다. 따라서 각 조사 대상에 대한 데이터 접근 범주를 확인하고 수집 및 분석을 위한 필요 권한와 인증 정보를 확보해야 한다.

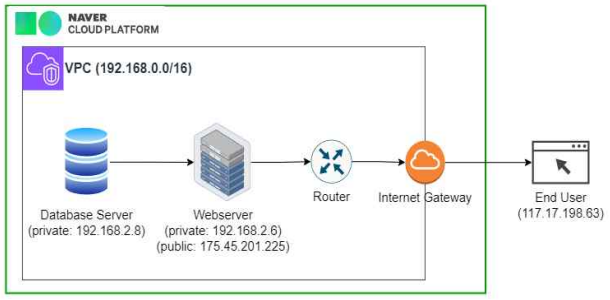
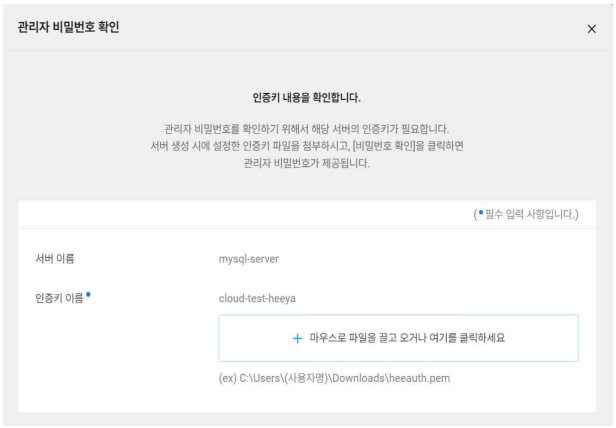


그림 3. 네이버 클라우드 기반 웹서비스 분석 환경 구성
Fig. 3. Configuration of the web service analysis environment based on Naver Cloud

먼저, 네이버 클라우드는 기본적으로 테넌트의 CPU, 메모리, 디스크, 네트워크 사용량에 대한 정보와 클라우드 플랫폼 내에서 수행한 인스턴스 생성, 공인 IP 할당, 서버 설치·삭제 등의 cloud activity 기록을 제공하므로 CSP의 협조를 우선적으로 요청할 필요는 없다.

CSU에서 리소스 사용 및 클라우드 활동 기록에 접근하기



*Figures are shown in the language supported by the target system, as they are based on actual screenshots captured during system operation.

그림 4. 네이버 클라우드 테넌트의 서버 접속 및 데이터 수집을 위한 인증키 입력 화면

Fig. 4. Authentication key input interface for server access and data collection in a Naver cloud tenant

위해서는 모든 권한을 소유하는 메인 계정이나 접근 권한을 소유하고 있는 서버 계정이 필요하다. 만약, 수사관이 네이버 클라우드에서 제공하는 API를 사용하여 데이터를 수집하려는 경우, API 인증키를 메인 계정을 통해 발급받거나 CSU에게 요청해야 한다. 또한, VPC 내 Webserver와 Database Server에 접근하여 서비스 관련 데이터를 수집하기 위해서는 각 서버에 접근·읽기 등의 권한을 가진 계정이 필요하다. 만약, 별도의 계정 관리를 하지 않았다면 관리자 계정이 필요하거나, 그림 4와 같이 네이버 클라우드에서 서버를 생성할 때 자동으로 설정하는 관리자 계정에 대한 정보를 수집하기 위한 테넌트의 인증키가 필요하다.

EU에서는 웹 브라우저를 이용한 서비스 이용 관련 데이터에 대한 수집이 필요하므로 웹 브라우저를 실행한 디바이스의 접속 계정이 필요하거나 물리적인 수집을 위해 디바이스 자체가 필요하다.

네이버 클라우드 기반 웹 서비스 조사를 위해 각 조사 대상별로 관련 데이터와 필요 권한을 정리하면 표 3과 같다.

표 3. 네이버 클라우드 도입 환경의 포렌식 조사를 위한 조사 대상별 관련 데이터 및 요구 권한

Table 3. Relevant data and required privileges by investigation target for forensic investigation in a Naver Cloud deployment environment

Target type	Related data	Required privileges
Cloud service user (CSU)	– Creation and access history of database servers and web servers, and usage records of related services – CPU, memory, and disk usage history – Artifacts related to the internal OS and file systems of database servers and web servers	– Naver Cloud tenant master account or privileges to access Cloud Activity and resources – Naver Cloud API authentication key – Privileges to access internal data such as the OS of database servers and web servers, or administrator account and authentication key (.pem)
End user (EU)	– Service access and usage logs of the web server	– Access privileges to the device running the web browser – Access privileges to web browser data

4-2 조사 대상별 관련 데이터 수집 단계

네이버 클라우드는 CSU에게 서버의 컴퓨팅 리소스 사용을 로깅하는 기본 모니터링(Basic Monitoring) 서비스와 클라우드 내 작업 활동을 로깅하는 Cloud Activity Tracer를 무료로 제공한다. CSU가 유료 제공되는 로깅 서비스인 Cloud Insight 서비스를 구독할 경우, 인스턴스된 프로세스, 서버 내 네트워크·파일시스템·메모리·네트워크 등과 같은 상세한 리소스 사용 정보가 로깅된다. 로깅된 데이터는 CSU의 메인 계정 접속을 거쳐 웹에서 수집하거나 네이버 클라우드에서 제공하는 REST API를 기반으로 도구를 제작하여 원격으로 수집할 수 있다. 이때, 네이버 클라우드의 REST API는 모든 서비스의 출력 결과는 JSON 형태로 반환된다[15],[16].

CSU가 네이버 클라우드에서 사용중인 인스턴스(Database Server, Webserver) 내 데이터는 CSU로부터 제공받은 계정과 인증키를 통해 원격으로 접속 가능하고, 접속 이후에는 기본 우분투 포렌식 데이터 수집 절차와 동일하게 논리적인 데이터 이미징 또는 데이터 복사를 통해 데이터를 수집한다.

EU의 디바이스에서는 기존 웹 브라우저 포렌식 절차 및 방법과 동일하게 Chrome 브라우저의 데이터 경로에서 히스토리, 쿠키, 캐시 등을 수집할 수 있다[17].

4-3 조사 대상별 관련 데이터 분석 단계

본 논문에서는 콘솔을 통해 레코드 단위로 수집한 네이버 클라우드의 3가지 로깅 서비스 데이터를 분석하였다. 그림 3의 데이터베이스 서버와 웹 서버를 주요 범주로 일주일간 로깅된 CPU, GPU, Memory 등의 리소스 사용 데이터를 분석하였다.

Cloud Activity Tracer는 태넌트의 서비스 내에서 수행된 모든 작업 내역을 그림 5와 같이 로깅한다. 그림 5는 웹 서버의 Network ACL Rule을 변경하고 공인 IP를 해제 및 할당 후 기록된 로그로, 각 작업 내역에 관해 작업 일시, 계정 구분, 리전, 작업 결과, 작업이 수행된 인스턴스 종류 등이 로그에 기록되는 것을 확인할 수 있다. 그림 3에서 구성한 웹 서비스에서 인스턴스 생성·삭제, 공인 IP 발급·할당·삭제, Network ACL Rule 변경 등의 보안 및 서비스 관리에 직결되는 행위를 수행 후 Cloud Activity Tracer 로그를 분석한 결과, 로그를 통해 관련 행위를 식별할 수 있었다. 이는 보안사고 발생 시 사고 원인을 규명하는 과정에서 유의미하게 활용될 수 있다.

작업 일시	작업 내역	작업 결과	상품명	계정구분
2023-11-14 20:35:01 (UTC+09:00)	Shutdown Server Instance	SUCCESS	Server	Main Account
2023-11-14 20:33:40 (UTC+09:00)	Update Network ACL Rule (Complete)	SUCCESS	VPC	Main Account
2023-11-14 20:33:25 (UTC+09:00)	Update Network ACL Rule (Request)	SUCCESS	VPC	Main Account
2023-11-14 20:23:58 (UTC+09:00)	associatePublicIp	SUCCESS	Server	Main Account
2023-11-14 20:23:44 (UTC+09:00)	Disassociate Public IP	SUCCESS	Server	Main Account

*Figures are shown in the language supported by the target system, as they are based on actual screenshots captured during system operation.

그림 5. 네이버 클라우드의 Cloud activity tracer 로그 내역
Fig. 5. Cloud activity tracer logs from Naver Cloud

Basic Monitoring의 로그 데이터에서는 분석 결과, 각 서버별로 CPU, GPU, Memory, Disk, Network 등 클라우드 자원의 시간에 따른 사용량에 대한 정보를 확인할 수 있었다. 이러한 기본 리소스 사용 모니터링 데이터는 급격한 자원 사용량 증가 시점, 네트워크 통신량 증가 시점을 확인하여 이상 발생 시점 및 상세 분석 지점을 파악하는 데 도움이 될 수 있다.

유료로 제공되는 Cloud Insight 서비스로 로깅된 데이터에서는 인스턴스 서버 내 프로세스 ID·이름·상태, 프로세스의 스레드 개수 변화, MAC/IP address 등의 정보를 확인할 수 있었다. 이뿐만 아니라 시스템의 CPU 사용 비율, 메모리 사용 비율, 메모리 페이지 In·Out 정보 등의 리소스 사용에 관한 상세한 변화가 로깅되는 것을 확인하였으며, 확인한 데이터는 보안사고 경위를 위한 행위를 식별하고 검증할 때 유용하게 활용될 가능성이 높다.

표 4는 Cloud Activity Tracer, Cloud Insight, Basic Monitoring(접속 경로: VPC/Server)의 로그 데이터 분석을 통해 식별할 수 있었던 사용자 행위를 나타낸다.

표 4. 네이버 클라우드 로그 내 사용자 행위 식별 결과
Table 4. User activities identified in Naver Cloud logs

Data name	Identifiable activity
Cloud activity tracer log	– Create/Login/Delete account – Create/Update/Delete VPC – Create/Update/Delete Server – Decryption/Reset Root Password – Create/Update Route Table – Create/Update/Delete Subnet – Create/Delete NW Interface – Create/Update/Delete AGC – Create/Update/Delete NWACL – Attach/Diassociate Public Domain/IP – Create/Delete Public IP – Subscribe To [Service name]
Cloud insight log	– CPU/IO wait ratio – CPU/interrupt ratio – CPU/system ratio – CPU/used ratio – MEMORY/page in·out – MEMORY/shared memory – MEMORY/swap – MEMORY/used memory – PROCESS/process ID·name·state – PROCESS/parent process ID – PROCESS/threads count – PROCESS/ps memory used ratio – SERVER/file system inodes used ratio – SERVER/disk write bytes average – SERVER/CPU interrupt ratio average – NETWORK/NIC MAC·IP address – NETWORK/send·receive packets per sec
Basic monitoring (VPC/server) log	– CPU used – Memory used – Disk used – Swap Used – Network In·Out – Disk Read·Write

V. 결 론

본 논문에서는 클라우드 컴퓨팅 서비스 도입 환경에서 보안사고 발생 시 포렌식 조사를 위해, 데이터 주체와 서비스 관점에서 조사 대상을 정의하고 클라우드 컴퓨팅 서비스 유형에 따른 분류와 특징을 정리하였다. 그리고 이를 기반으로 한 클라우드 컴퓨팅 서비스 보안사고 포렌식 조사 프레임워크를 제안하였다. 그리고 국내 상용 클라우드 서비스인 네이버 클라우드에서 웹 서비스 환경을 구축하고 제안하는 클라우드 컴퓨팅 서비스 보안사고 포렌식 조사 프레임워크에 따라 분석을 수행함으로써 실제적인 적용에 대한 분석 결과를 보였다.

제안한 프레임워크는 Cloud Service Provider(CSP)의 협조를 기본 전제하는 것이 아닌, 협조 요청 필요성과 협조 여부를 고려하고 이에 따른 조사 절차를 구분함에 따라, 기존 클라우드 컴퓨팅 포렌식 프레임워크보다 실질적 조사 상황을 고려하였다. 이는 CSP 협조 여부에 의존하지 않는 유연한 조사 절차로 현실적인 제약 환경에서도 조사의 일관성을 확보할 수 있을 것으로 기대된다.

또한, 클라우드 컴퓨팅 서비스 자체만을 범주로 하는 기존 연구와 달리, 본 프레임워크는 클라우드 컴퓨팅 서비스를 도입하여 제공하는 실제 서비스까지 범주를 확대하고 실제 서비스의 최종 사용자까지 조사 범주에 포함한다. 이에 따라, 다양한 출처의 증거를 통합적으로 분석함에 따라 행위 간 인과관계 및 보안사고 발생 과정을 보다 정밀하게 재구성할 수 있고, 전반적인 포렌식 분석의 신뢰성과 정확도를 향상시킬 수 있다.

클라우드 컴퓨팅 서비스 도입 환경에서 보안사고 발생 시, 본 논문에서 제안하는 절차와 같이 CSP, CSU, EU에 대한 종합적인 분석이 정상적으로 수행하기 위해서는 대상 클라우드 서비스 환경의 인증 체계와 데이터 관리에 대한 이해를 기반으로 필요 권한과 인증 정보(비밀키), 계정 정보에 대한 사전 준비나 협의가 원활하게 수행되는 것이 중요하다. 특히, 법집행기관의 수사 관점에서 사고조사를 위한 준비 단계에서 필요한 정보 제공을 강제해야 할 경우 대상 클라우드 서비스 환경에 대한 사전 이해나 분석이 필요하다. 이에 따라 향후 제안하는 클라우드 보안사고 포렌식 조사 프레임워크를 기반으로 한 여러 클라우드 컴퓨팅 서비스에 대한 포렌식 분석 연구를 수행하고자 한다.

참고문헌

[1] Public Cloud Promotion Center. Cloud Transition for Government and Public Institution - Background and Necessity [Internet]. Available: https://saas.go.kr/govcloud/mainpage/switchproject-introduce/project1_2.

[2] Check Point Research, 2023 Cyber Security Report, Chapter 3. Cloud: Third Party Threat, pp. 41-42, 2023

[3] Ministry of Science and ICT. Cloud Computing Development and User Protection Act [Internet]. Available: http://www.yeslaw.com/lims/front/page/fulltext.html?pAct=view&pPromulgationNo=196402.

[4] Korea Internet and Security Agency. Guide to the Cloud Security Assurance Program (CSAP) [Internet]. Available: https://isms.kisa.or.kr/main/csap/notice/?boardId=bbs_0000000000000004&mode=view&cntId=62.

[5] National Intelligence Service and National Security Research Institute. National Cloud Computing Security Guidelines [Internet]. Available: https://www.ncsc.go.kr:4018/main/cop/bbs/selectBoardArticle.do?bbsId=InstructionGuide_main&nttId=18590&pageIndex=1.

[6] National Intelligence Service. 2023 National Information Security White Paper (Korean Version) [Internet]. Available: https://www.kisa.or.kr/20303/form?postSeq=12003&lang_type=KO.

[7] S. Alqahtany, N. Clarke, S. Furnell, and C. Reich, "Cloud Forensics: A Review of Challenges, Solutions and Open Problems," in *Proceedings of the 2015 International Conference on Cloud Computing (ICCC),* Riyadh, Saudi Arabia, pp. 1-9, 2015

[8] J. J. Shah and L. G. Malik, "Cloud Forensics: Issues and Challenges," in *Proceedings of the 2013 6th International Conference on Emerging Trends in Engineering and Technology,* Nagpur, India, pp. 138-139, 2013.

[9] M. E. Alex and R. Kishore, "Forensics Framework for Cloud Computing," *Computers & Electrical Engineering*, Vol. 60, pp. 193-205, 2017. https://doi.org/10.1016/j.compeleceng.2017.02.006.

[10] K. Park and S. Noh, "Investigation Methods from a Forensic Perspective for Cloud Services," *Journal of the Korea Industrial Information Systems Society*, Vol. 17, No. 1, pp. 39-46, February 2012. https://doi.org/10.9723/jksiis.2012.17.1.039

[11] J. Park, J. Park, M. Kim, and E. Heo, "A Study on a Reference Model for Cloud Forensics," in *Proceedings of the Korea Institute of Communications and Information Sciences Conference*, Jeju, pp. 1678-1679, 2017.

[12] I. Jung, J. Oh, J. Park, and S. Lee, "A Digital Forensic Study on IaaS-Type Cloud Computing Services," *Journal of the Korea Institute of Information Security & Cryptology*, Vol. 21, No. 6, pp. 55-65, 2011. https://doi.org/10.13089/JKIISC.2011.21.6.55

[13] P. Sanda, D. Pawar, and V. Radha, "An Insight into Cloud Forensic Readiness by Leading Cloud Service Providers: A Survey," *Computing*, Vol. 104, No. 9, pp. 2005-2030, 2022. https://doi.org/10.1007/s00607-022-01077-2

[14] National Intelligence Service and National Security Research Institute, Cloud Computing Classification, in National Cloud Computing Security Guidelines, pp. 7-9. 2023.

[15] NCloud API. GetActivityList [Internet]. Available: https://api.ncloud-docs.com/docs/management-cloudactivitytracer-getactivitylist.

[16] NCloud API. Cloud Insight API Overview [Internet]. Available: https://api.ncloud-docs.com/docs/management-cloudinsight.

[17] R. Nelson, A. Shukla, and C. Smith, Web Browser Forensics in Google Chrome, Mozilla Firefox, and the Tor Browser Bundle, in *Digital Forensic Education: An Experiential Learning Approach*, Cham, Switzerland: Springer International Publishing, pp. 219-241, 2020.

서승희(Seunghee Seo)

2017년 : 서울과학기술대학교(공학학사)
2019년 : 서울과학기술대학교 대학원 (공학석사)
2024년 : 서울과학기술대학교 대학원 (공학박사-컴퓨터공학)
2024년~현 재: 한국전자통신연구원 부설 연구소 연구원
※관심분야 : 정보보호(Information Security), 디지털포렌식(Digital Forensics) 등