정 보 보 호 학 회 지
제 31 권 제3호, 2021. 6

퍼블릭 클라우드에서 자동화 IR(Incident Response)를 통한 보안 향상 기술

김 대 협*, 한 현 상**, 박 문 형***, 장 항 배*

요 약

클라우드 컴퓨팅은 사용자들의 직접적인 인프라 관리 없이 가상 스토리지, 네트워크, 컴퓨팅 리소스 등을 빠르게 고객에게 제공해주는 서비스이다. 클라우드 컴퓨팅은 누구나 외부에서 접근할 수 있으며 운영 담당자가 모든 클라우드 인프라를 직접 관리하기 어렵기 때문에 보안이 기존 인프라 보안과는 차별화된 운영 방법이 필요하다. 또한, 관리자가 온프레미스 기존의 사고 대응 프로세스를 클라우드 인프라에 적용하기에는 리소스 부족, 사고확산방지, 포렌식 등이 논리적, 물리적으로 어려움이 존재하여 클라우드 환경에서 적용가능한 자동화된 IR(Incident Response)의 모델을 설계하여 자동화된 사고대응 프로세스를 새롭게 제안 한다.

Ⅰ. 서 론

오늘날 클라우드 컴퓨팅은 민간분야의 웹사이트, 서비스 관리, 데이터 저장 장소에서부터 시작하여 쇼핑몰 등 다양한 어플리케이션 서비스에 사용이 되고 있다. 이러한 클라우드 컴퓨팅은 누구나 접근이 가능한 가상의 클라우드 공간에 컴퓨팅 리소스를 배포한다는 점에서 초기 도입비용, 인프라 관리 비용, 그리고 일관된 서비스를 제공해 줄 수 있다는 장점이 존재한다. 특히 대한민국은 클라우드를 다양한 보안 정책으로 인하여 늦게 도입을 하고 있지만 세계적으로 여러 기업이 클라우드를 업무에 도입함에 따라서 마찬가지로 이용이 증가하고 있다. 가트너[1]에 따르면 2019년 전체 클라우드 시장 규모는 약 2426억 달러 였다. 2020년에는 2019년도 보다 6% 성장하여 약 2575억 달러 규모에 도달 했다. 2021년에는 시장 규모가 2020의 18%인 3049억 달러로 증가하는 것을 알 수 있고, 2022년 예측으로는 3622억 달러로 2021년보다 19%정도 증가할 것이라예측 하고 있다, 이에 따라서 매년 클라우드 시장의 규모는 지속적으로 높게 증가되고 있는 것을 알 수 있으며, 이에 따라서 클라우드에 저장된 데이터양, 네트워크, 클라우드 활용 범위가 점차 넓어지고 있다.

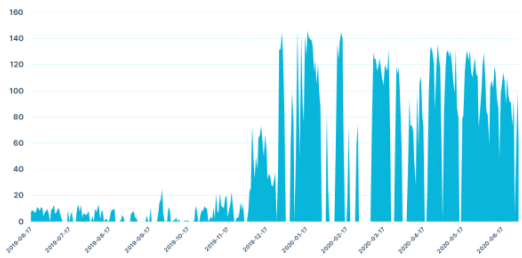
	2019	2020	2021	2022
Cloud Business Process Services (BPaaS)	45,212	44,741	47,521	50,336
Cloud Application Infrastructure Services (PaaS)	37,512	43,823	55,486	68,964
Cloud Application Services (SaaS)	102,064	101,480	117,773	138,261
Cloud Management and Security Services	12,836	14,880	17,001	19,934
Cloud System Infrastructure Services (IaaS)	44,457	51,421	65,264	82,225
Desktop as a Service (DaaS)	616	1,204	1,945	2,542
Total Market	**242,696**	**257,549**	**304,990**	**362,263**

〔그림 1〕 전 세계 공용 클라우드 서비스 최종 사용자 지출 예측(백만 달러)

국내에서도 2019년도에 금융위원회가 금융 분야에서의 클라우드 이용을 장려하고 촉진하기 위하여 클라우드와 관련한 전자금융감독규정의 일부 규제를 개정하고 금융분야 클라우드컴퓨팅 서비스 가이드 개정·배포를 하여 정보가 민감한 금융 분야에서의 클라우드 사용사례 또한 증가하고 있다[2].

하지만 이러한 클라우드 이용률이 높아지는 것과 대비하여, 클라우드 보안 사고도 지속적으로 증가해왔다. 특히 2019년 6월부터 2020년 7월까지 16,371건의

* 중앙대학교 융합보안학과 (대학원생, anonyges@cau.ac.kr; 교수, hbchang@cau.ac.kr)
** Amazon Web Services사 Security & Risk Compliance팀 (Consultant, misadz@naver.com)
*** 극동대학교 과학기술대학 해킹보안학과 (강사, mhpark@kdu.ac.kr)



〔그림 2〕 허니팟에 대한 공격의 양 (클라우드)

공격을 추적하고 분석 한 Aqua Security의 “2020 Cloud Native Threat Report”[3]에 따르면, 클라우드 시스템에 대한 공격은 전년보다 공격이 연초에 250% 증가 했다.

특히 보안에 민감한 회사가 클라우드 서비스를 이용하게 되면서 내·외부의 요인 보안 위협이 발생할 수 있다. 클라우드는 온 프레미스보다 가용성 리스크가 없다고 알려졌지만, 종종 장애, 중단 등이 발생하기도 한다. 또한, 운영자의 클라우드 운영 미흡이나 클라우드 서비스 제공자(CSP, Cloud Service Provied)의 기술적 오류로 인하여 중단, 장애가 발생할 수 있다[4]. 최근에 국내에 있는 POP(Point of Presence)서버를 사용하지 않고 해외에 있는 POP서버를 사용하게 되어서 국내의 데이터가 해외에 저장되는 컴플라이언스 위반도 발생할 가능성이 있다. 특히 국내 컴플라이언스는 해외의 컴플라이언스 기준과 다르기 때문에 국내 컴플라이언스 기준을 준수하지 못하는 상황이 발생될 수 있다. 특히 급변하는 국가 간의 정치 문제, 또는 CSP가 국내에 있지 않아 일부 협조 거부 등으로 인해 위협이 발생 될 수 있다. 특히 보안 위험은 해킹, 개인 정보 유출 등 사이버 공격으로 인한 피해가 존재할 수 있으며 클라우드 환경에 대한 전문성 결여, 설정 부주의 등으로 인해 발생할 수 있다.

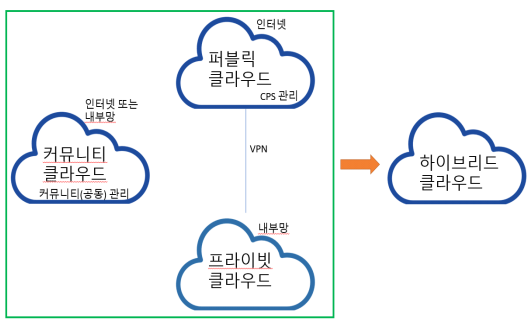
Ⅱ. 관련 연구

2.1. 클라우드 컴퓨팅

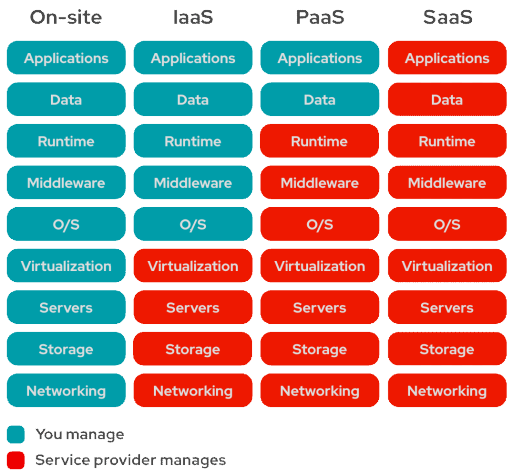
먼저 클라우드 서비스란 기존의 온-프레미스(On-Premise) 환경의 네트워크, 서버, 스토리지의 인프라에서 확장하여 가상화 기술을 통해 애플리케이션, 서비스, 등 다양한 컴퓨팅 자원을 언제 어디서나 사용자가 필요 할 때 퍼블릭/사설 네트워크를 통해 제공하는 방식의 기술 이다[5].

클라우드는 배포 모델에 따라서 3가지 경우의 수가 있는데 이는 각각 퍼블릭 클라우드(public cloud), 프라이빗 클라우드(private cloud), 커뮤니티 클라우드(community cloud), 하이브리드 클라우드(hybrid cloud) 이다[6]. 퍼블릭 클라우드는 누구나 접근할 수 있는 퍼블릭 네트워크에 클라우드 컴퓨터가 프로비저닝(provisioning)된 클라우드이다. 현재는 소기업, 중소기업, 대기업, 학교, 정부 기관, 등 다양한 기업에서 운영하고 있다. 프라이빗 클라우드는 퍼블릭 클라우드와 다르게 외부에서 접근을 제안해야 되는 단일 기업 등에서 독점으로 사용하는 클라우드이다. 이는 보통 정보에 민감한 기업에 의하여 운영 된다. 따라서 클라우드 서버의 위치가 보통 온프레미스(on- premise)로 운영되나 오프프레미스(off-premise)방식도 존재한다. 커뮤니티 클라우드는 보안 요구사항, 정책, 컴플라이언스 등 다수의 공통 목적을 위해 내부 또는 제 3자가 운영하는 클라우드이다. 하이브리드 클라우드는 퍼블릭 클라우드와 프라이빗 클라우드 또는 커뮤니티 클라우드의 모델을 2개 이상 같이 운영하는 모델 이다. 이는 보통 퍼블릭 클라우드에서 서비스를 제공하지만 민감한 데이터를 보관해야 될 경우가 필요할 때 프라이빗 클라우드에 저장하는 방식으로 진행할 수 있게 구성한 것이 하이브리드 클라우드이다.

대표적인 클라우드 서비스 모델은 클라우드가 어떤 방식으로 이용자 또는 사용자에게 서비스되는지를 나타낸다. 클라우드 서비스 모델은 SaaS(Software as a Service), PaaS(Platform as a Service), IaaS(Infrastructure as a Service)가 존재 한다[7]. SaaS 사용자가 클라우드 인프라를 네트워크, 자원 사용률(CPU, 메모리, 등)을 관리할 필요 없이 CSP가 클라우드 인프라에서 운영하는 애플리케이션을 이용하는 방



〔그림 3〕 클라우드 모델 종류



〔그림 4〕 온프레미스와 클라우드 서비스 모델 유형

식이다. SaaS 이용자는 다양한 단말기에서 SaaS 클라우드 환경에 접근 가능한다. 이러한 SaaS의 대표적인 서비스로는 Microsoft사의 Office365 제품이 있다. 또한, SECaaS (SECurity as a Service)라는 서비스 등 다양한 서비스가 존재 한다.

그다음 단계로는 PaaS라는 서비스 모델이 존재한다. PaaS는 CSP가 제공하는 클라우드 인프라에 사용자가 개발 또는 구입한 애플리케이션을 설치 또는 디플로이하여 운영하는 방식이다. 사용자는 애플리케이션 데이터, 개인 정보, 데이터, 등을 관리해야 하지만 CPU, 메모리, 네트워크, 운영체제, 스토리지 등 인프라의 자원을 관리할 필요는 없다.

가장 온 프레미스와 비슷한 IaaS는 스토리지, 네트워크, OS, 미들웨어, 애플리케이션 등 거의 CSP의 컴퓨팅 자원을 클라우드 서비스 사용자가 프로비저닝하는 방식이다. 온 프레미스 환경과 비슷하게 대부분의 컴퓨팅 자원 관리는 가능하지만, 인프라 레벨의 하드웨어적 자원 관리는 불가능한다. 하지만 가상으로 이루어져 있는 운영체제, 네트워크, 스토리지, 애플리케이션, 메모리, 등 대부분의 가상 구성요소 클라우드 인프라를 관리하고 통제할 수 있다.

2.2. 클라우드 컴퓨팅 보안 위협

기존의 클라우드 서비스 이용 확대, 중요 또는 민감정보의 클라우드 저장, 등 민감한 정보들이 클라우드에서 운영되기 시작하여 이에 따른 사이버 공격도 점차

〔표 1〕 클라우드 보안 위협과 구분

범주 구분	위협의 예	위협 구분
가상화 문제	VM 탈출 악성코드, 호핑, 이미지 변조, 하이퍼바이저 기반 루트킷	클라우드 공유자원
중복된 신뢰 경계	Multi Tenancy로 인한 보안 경계의 중첩	
네트워크 침입	네트워크 트래픽 도 감청, 악의적인 중간자	기존의 보안 문제와 동일
서비스 공격	서비스 왜곡, 래핑, 스캐닝	
권한 탈취	접근 권한의 위 변조, 식별자 관리 익명화	
과부하 공격	DoS, DDoS, 리소스 점유	
구현오류	설계 결함 및 설정 결함 등을 취약점으로 악용	
관리문제	내부 설정 오류 및 미흡	

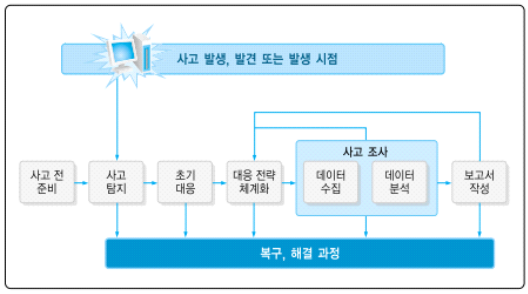
증가하고 있다. 특히 클라우드 보안에 대한 위협과 구분은 아래 표처럼 나뉠 수 있다[8].

특히 클라우드는 누구나 접근할 수 있으므로 설정 오류로 인한 위험이 존재 한다. 이는 클라우드 애플리케이션 내에 있는 데이터에 대한 가시성 부족으로 인하여 악의적인 행위자에 의한 클라우드 애플리케이션의 데이터 도용이 가능 하다[9]. 특히 권한 설정에 민감한 데이터에 액세스할 수 있는 사람에 대한 불완전한 제어. 사람이 항상 클라우드 애플리케이션과 주고받는 데이터를 모니터링할 수 없다. 클라우드 애플리케이션의 보안 관리 기술을 갖춘 직원 부족으로 인한 관리적 위험이 대두되고 있다. 또한 악의적인 내부자 절도 또는 데이터 오용을 방지할 수 없다[10].

2.3. 수동 사고 대응 방법론

예전부터 인터넷 범죄의 증가로 인해 CSIRT (Computer Security Incident Response Team)가 중요한 역할을 수행하고 있으며, 현재 온 프레미스 관련 환경에서는 CERT(Computer Emergency Response Team), 보안관제사 등 다양한 보안 팀이 존재하고 있다. 이는 전 세계 선진국 기업이 현재 운영 중인 시스템이다. 현재 온 프레미스에서 사고 대응 단계는 7단계로 나뉘어져 있다[11]. 이는 아래와 같다.

- 사고 전 준비 과정 : 사고가 발생하기 전 다양한 보



〔그림 5〕 사고 대응 7단계

안 솔루션, 보안 장비를 이용하여 침해 사고 대응팀과 조직적인 대응을 준비

- 사고 탐지 : 보안 솔루션과, 정보보호 및 네트워크 보안 장비에 의한 이상 징후 탐지, 패턴 탐지로 인하여 보안 관리자에 의한 침해 사고의 식별
- 초기 대응 : 사고 초기 조사 수행, 사고 기본적인 세부사항 기록, 사고대응팀(CERT) 신고 및 소집, 침해사고 관련 부서에 통지
- 대응 전략 체계화 : 최적의 전략을 프로세스를 결정하고 관리자 승인을 획득, 초기 조사 결과를 참고하여 소송이 필요한 사항인지를 결정하여 사고 조사 과정에 수사기관 공조 여부를 판단
- 사고 조사 : 다양한 보안 장비에서 데이터 수집 및 사고 관련 데이터 분석을 통하여 사고 조사, IOC(Indicator of Compromise) 검색, 이후 피해 확산 및 사고 재발을 어떻게 방지할 것인지를 프로세스 설립
- 보고서 작성 : 사고 대응, 피해, 프로세스 결과 보고서 작성
- 해결 : 이후 유사 공격을 예방하기 위한 보안 정책의 수립 변경, 절차 변경, 기록, 장기 보안 정책 수립, 기술 수정 계획 수립 등

Ⅲ. 자동화 IR(Incident Response)를 이용한 보안 향상 기술

클라우드 사용자가 지속적으로 늘어남에 따라서 클라우드 관련 사이버 공격과 범죄도 나날히 증가하고 있다. 하지만 보안 담당자가 수동으로 이러한 사고에 대응하게 된다면 아래와 같이 식별부터 사고 분석의 시간이 많이 소요되는 것을 알 수 있다. 특히 보안인프라 담당자은 인프라관리, 사고분석의 업무로 상당한 대

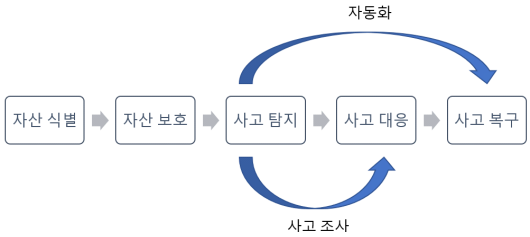
〔표 2〕 보안담당자의 침해 사고에 대한 IR을 수동으로 할 시 소요 시간

해야될 일	MTTR (평균대응시간)
SIEM, NGFW, EPP, EDR, Proxy 장비에서 이벤트 생성	5분
영향을 받는 자산 확인 - 서버, 서비스	5-10분
위협 인텔리전스 피드에 대한 IOC 확인	5분
앞에서 발생한 보안 사고 데이터의 상관관계 분석	10-20분
수동 데이터 조사	10분-1시간
보안사고 업무 추적	10분-1시간
감사 추적 및 로깅 유지	지속적

응 시간이 소요되는 것을 알 수 있다.

특히 시간이 많이 소요되는 수동 데이터 조사에는 네트워크 기반 증거, IDS 로그 수집, 라우터 로그 수집, NGFW 로그 수집, Syslog 수집, 등 다양 로그 수집을 보안담당자가 해야 한다. 또한, 호스트 기반 증거 수집도 병행되어야 하는데 이는 휘발성 메모리 데이터 수집, 피해 시스템의 의심스러운 파일 수집, 디스크 백업 수집, 이벤트 파일 수집, 등이 있다. 이러한 수많은 증거 수집은 보안담당자가 하기에 부담이 되고 많은 시간 소요가 필요한다. 또한 보고서를 위하여 양식에 맞추어서 작성을 해야 하며 로깅도 지속적으로 모니터링이 필요한다. 이에 따라 현재 연구에서는 퍼블릭 클라우드의 자동화 IR(Incident Response)를 통한 보안 모델을 설계하여서 더욱더 빠른 사고 대응을 할 수 있는 보안 향상 방안 연구를 진행했다.

첫 번째 클라우드 자동화 IR의 핵심은 어느 부분을 자동화 해야할지 범위를 지정하는 것이다. 보통 IR의 범위는 자산 식별, 자산 보호, 사고 탐지, 사고 대응, 사고 복구로 분류 한다. 자산 식별에서는 환경 내의 클라우드 리소스, 애플리케이션 및 데이터를 식별하고 이해한다. 자산 보호에서는 서비스 제공을 하기 위해 보안 제어 및 보호 장치를 개발하고 사용한다. 이 부분에서는 타 정보보호 솔루션을 사용하여서 구현한다. 사고 탐지에서는 공격자가 침입하였을 시 사이버보안 이벤트 발생을 식별하는 단계이다. 사고 조사에서는 보안 이벤트에 대한 체계적인 검사를 수행하여 RCA(Root Cause Analysis)를 진행하여 원인 파악을 한다. 대응에서는 감지된 보안 이벤트에 대해 자동 또는 수동으로



〔그림 6〕 클라우드 자동화 IR 범위

조치한다. 복구 단계에서는 공격자로 인해 손상된 기능 또는 서비스를 복원한다.

두 번째 클라우드 자동화 IR의 핵심은, 어떠한 트리거를 통하여 최초 사고를 식별하고 탐지하는지에 대한 사고 지표를 구성하고 식별하는 단계이다. 클라우드 네이티브 솔루션 및 제3자 애플리케이션도 마켓에 있는 솔루션을 활용하여 클라우드 인프라의 사고를 식별 및 탐지하기 위하여 구성하며 솔루션을 통하여 어떠한 자산을 보호할 것인지, 또는 어떠한 로그를 수집할 것인지, 어느 저장소에 로그를 저장할 것인지 또는 퍼블릭 클라우드 만의 로그 저장소를 이용할 것인지 파악해야 한다.

세 번째로, 클라우드 자동화 IR의 범위와 자산이 식별되었다면 자동화된 사고대응 프로세스를 구성하는 것이다. 클라우드는 프로비저닝이 간편하고 서비스 의 연동이 API를 통하여 빠르게 정의가 가능하고 이를 통한 자동화 프로세스를 구성하기 용이하고 이로 하여금 사고발생 인프라에 대한 식별, 격리, 분석, 복구, 데이터 형상관리가 가능한다. 아울러 자동화 IR 범위를 전사적인 컴프라이언스로 구성하여 사고 대응 프로세스가 구성될 수 있는 아키텍쳐를 적용하도록 한다.

이러한 클라우드 자동화 IR 모델을 적용하면 기존 보안담당자가 수행하는 사고 대응보다 빠르게 사고 대

〔표 3〕 로그 탐지 및 분석에 필요한 자산

DoS. DDoS	웹 취약점	비인가 접근	악성코드
FW	NGFW	IAM	Sandbox
Load Balancer	UTM	Key 관리	AV Wall
WAF	IPS	DLP	NGFW
서비스 서버	IDS	CASB	GuardDuty
	WAF	CWPP	
	DB 서버	CSPM	

〔그림 7〕 클라우드 자동화 IR 모델 (서비스 우선순위)

〔표 4〕 침해 사고에 대한 클라우드 자동화 IR을 사용할 시 소요 시간

해야될 일	MTTR (평균대응시간)
SIEM, NGFW, EPP, EDR, Proxy 장비에서 이벤트 생성	1분
영향을 받는 자산 확인 - 서버, 서비스	1분
위협 인텔리전스 피드에 대한 IOC 확인	1분
앞에서 발생한 보안 사고 데이터의 상관관계 분석	5분
자동 데이터 조사	5분
보안사고 업무 추적	5분
감사 추적 및 로깅 유지	지속적

응을 할 수 있는 것으로 판단된다.

Ⅳ. 결 론

최근 클라우드 컴퓨팅은 회사, 업계 및 기타 여러 분야의 서비스와 통합되어 활발히 연구가 진행되고 있으며, 민간분야에서부터 군사 분야까지 다양한 분야에서 활용이 되고 있다. 이러한 클라우드 컴퓨팅은 누구나 접근이 가능한 가상의 클라우드 공간에 컴퓨팅 리소스를 배포한다는 점에서 초기 도입비용, 인프라 관리 비용, 그리고 일관된 서비스를 제공해 줄 수 있다는 장

점이 존재한다. 특히 대한민국은 클라우드를 다양한 보안 정책으로 인하여 늦게 도입을 하고 있지만, 세계적으로 여러 기업이 클라우드를 업무에 도입함에 따라서 마찬가지로 이용이 증가하고 있다. 현재 온 프래미스 또는 클라우드 환경에서 보안담당자가 수동으로 사고를 대응하고 있다. 이는 급변하는 클라우드 환경에서 수동으로 사고 대응, 분석을 진행함에 따라서 사고 대응 속도가 즉시 수행될 수 없으며, 식별 및 인지가 어렵다는 것을 확인할 수 있다. 이에 따라서 본 연구에서는 클라우드 자동화 IR 모델을 설계하여 기존의 보안 담당자가 수동으로 사고에 대응하는 시간을 클라우드 인프라에서 적용 가능하도록 제안하여 다양한 사고를 식별하고 자동화된 대응 프로세스를 적용하여 불필요한 리소스를 제한하고, 언제든지 사고에 대응할 수 있는 방법을 제시 한다.

참 고 문 헌

[1] 가트너, “Gartner Forecasts Worldwide Public Cloud End-User Spending to Grow 18% in 2021”, Nov, 2020

[2] 금융위원회, “클라우드와 금융혁신“, May 2019

[3] Aquasec, “2020 Cloud Native Threat Report”, pp. 6, Sep 2020.

[4] KFTC, Cloud Computing Challenges, pp. 33~54, 2011

[5] SW·Computing Cloud Computing, TTA, PP. 67~151, 2019

[6] Hofmann, P., & Woods, D, "Cloud computing: the limits of public clouds for business applications", IEEE Internet Computing, Vol. 14, No. 6, pp. 90-93, Nov.-Dec. 2010.

[7] Analyze the status of cloud services in the financial sector, FSEC, pp. 34~57, 2015

[8] D. H. Kim, J. H. Lee, & Y. P. Park, "A Study of Factors Affecting the Adoption of Cloud Computing", Society for e-Business Studies, Vol. 17, No. 1, pp. 111-136, February 2012.

[9] 한국클라우드보안협회, CSA Summit Korea 2013, 삼정KPMG경제연구원. “클라우드 컴퓨팅 개념과 산업동향”, 2016

[10] KISA, Cloud Information Protection Guide, pp. 1~66, 2017

[11] KISA, 제2010-8호-침해사고 분석 절차, pp.12-29, 2010

〈저 자 소 개〉

김 대 협 (DaeHyeob Kim)

2017년~현재 : 중앙대학교 융합보안학과 석사과정

2020년~현재 : Fortinet Korea SE팀 Consultant

<관심분야> 클라우드, 정보보호, 인공지능

한 현 상 (HyeonSang Han)

2019년 2월 : 성균관대학교 정보통신대학원 정보보호학 공학석사

2020년~현재 : Amazon Web Services사 Security & Risk Compliance팀 Consultant

<관심분야> 클라우드, 침해사고 대응, 네트워크 보안

박 문 형 (Moonhyung Park)

2003년 8월 : 강원대학교 경영대학 경영학사

2008년 8월 : 건국대학교 정보통신대학원 정보보호학 공학석사

2019년 3월~현재 : 극동대학교 해킹보안학과 강사

<관심분야> 클라우드 보안, 엔드포인트 보안, 정보보안

장 항 배 (Hangbae Chang)

종신회원

2006년 : 연세대학교 정보시스템관리 박사

2014년~현재 : 중앙대학교 산업보안학과 정교수

<관심분야> 중소기업 정보보호, 정보오남용 및 유출방지, 성과분석 체계