특집 06

Public 클라우드 컴퓨팅 환경에서 통합보안관제를 위한 아키텍처 설계

김영희 (한국폴리텍대학)

목 차

1. 서 론
2. Public 클라우드 컴퓨팅 환경에서 보안 위협
3. Public 클라우드 통합 보안관제 모델
4. 결 론

1. 서 론

클라우드 컴퓨팅은 기업에서 사용되는 IT자원 및 시스템을 사용자 필요에 따라 대여하여 적시에 네트워크를 통해 이용하는 컴퓨팅 환경이다. 과거 대부분 기업들의 IT 환경은 시스템을 IDC 또는 전산실 내 고정적인 장소에 구성하고 운영하는 On-Premise 환경이었다면, 최근 각광받고 있는 클라우드 컴퓨팅 서비스는 IT 자원 사용에 대한 효율성 증대를 목적으로 초기 구축비용을 낮추고 필요 시 필요한 만큼 임대하여 사용하는 방법이다. 4차 산업 혁명에 따른 현재 기업들은 변화에 민첩하게 대응하는 유연한 인프라 기반 구성에 대한 필요성과 제약 없는 IT 자원 활용, 비용 효과적이고 보다 효율적인 서비스 개발 및 운영환경 구현이 필수적으로 요구되는 상황이다. 이에 발맞춰 클라우드 컴퓨팅 서비스가 유연성, 확장성을 중심으로 기술이 빠르게 발전함에 따라 컨테이너, 쿠버네티스, MSA 아키텍처 구현 등을 통해 보다 효율적 서비스 개발이 가능하고 비용 효율적이고, IT 시스템 변경에 대한 빠른 의사결정이 가능한 특성 때문에 빠르게 확산되고 있다[1]. 클라우드 컴퓨팅은 제공 형태별로 프라이빗 클라우드(Private Cloud), 퍼블릭 클라우드(Public Cloud), 하이브리드 클라우드(Hybrid Cloud)로 구분되고 컴퓨팅 활용도에 따른 SaaS(Software as a Service), IaaS (Infrastructure as a Service), PaaS(Platform as a Service)와 같은 유형으로 분류된다[2]. 해당 서비스의 경우 대표적으로 아마존, 구글, 마이크로소프트와 국내 네이버, KT등 다양한 사업자가 상용서비스를 제공하고 있으며, 자체적으로 보안위협에 대응하기 위해 클라우드 컴퓨팅 환경에 특화된 보안서비스를 함께 제공하고 있다[3,4]. 하지만, 클라우드 컴퓨팅 환경의 경우 기존의 On-Premise 환경에서 발생되는 보안 위협과 함께 클라우드 환경 특성에 따른 새로운 형태의 보안 위협이 대두되고 있으며, 클라우드 서비스 사업자가 제공하고 있는 보안 서비스 활용 시 기존 On-Premise 환경에서 구축 운영 중인 보안관제 체계등과의 상이함에 따라 통합관리가 어려운 상황이다. 이에 클라우드 컴퓨팅 서비스 환경에서 발생하는 보안 위협을 효과적으로 대응하고 기존 보안관제 체계와의 통합 및 연동을 통한 통합보안 관제체계가 필요한 실정이다.

본 연구에서는 클라우드 컴퓨팅 환경에서의 새로운 위협 분석과 기존의 On-Premise 환경에서의 보안관제 체계를 바탕으로 Legacy/Public 클라우드 환경을 고려하여 기존에 구축된 보안관제시스템을 활용해 좀 더 유연하고 효과적으로 보안위협을 대응할 수 있는 클라우드 컴퓨팅 환경 구성을 위해 내부·외부망의 접근 통제 및 보안 위협 대응을 위한 별도의 Security Zone을 구성하고 On-Premise 환경에서 운영 중인 보안관제 체계와 연동을 위한 클라우드 통합보안관제 아키텍처를 제안한다.

2. Public 클라우드 컴퓨팅 환경에서 보안 위협

기업의 경우 디지털 혁신을 위한 클라우드 전환이 가속화되면서, On-Premise 환경에서는 경험하지 못했던 새로운 보안 위협과 Public 클라우드 환경의 특성 상 공격자가 침투할 수 있는 경로가 더 다양해지고, 관리 대상 증가로 클라우드 컴퓨팅 서비스 도입에 따른 보안 가시성 확보가 어려워지고 있다. 이에, CSA(Cloud Security Alliance)에서는 매년 보안전문가의 설문을 통해 클라우드 컴퓨팅 환경에 발생되는 보안 위협을 매년 선정하고 있다. 해당 위협의 경우 기술적 위협으로 안전하지 않은 API, 가상화 공유 기술 취약점, 계정·서비스 및 트래픽 탈취, 데이터 유출 (Data Breaches), 데이터 손실 (Data Loss), 시스템 취약점, 서비스 거부 (DoS: Denial of Service) 공격 등을 대표적인 위협으로 분류하고, 관리적 위협으로 클라우드 컴퓨팅 남용 또는 악용, 악의적인 내부자들, 공개되지 않은 위협, 불충분한 실사, 불충분한 식별자, 권한 및 접근관리 등 On-Premise 환경의 보안 위협과 유사한 형태의 위협과 클라라우드 환경의 특성 상 자원공유 환경에서 발생되는 정보 위탁, 가상화등에 따른 복합적인 보안 위협이 추가적으로 발생되고 있다[5,6]. 관련 위협 현황은 <표 1>과 같다.

〈표 1〉 CSA 보안 위협 현황

구분	내용
기술적 위협	안전하지 않은 API (App Programming Interface)
	가상화 공유 기술 취약점
	계정, 서비스 및 트래픽 탈취
	데이터 유출 (Data Breaches)
	데이터 손실 (Data Loss)
	서비스 거부 (DoS: Denial of Service)
	시스템 취약점
관리적 위협	클라우드 컴퓨팅 남용 또는 악용
	악의적인 내부자들
	공개되지 않은 위협
	불충분한 실사
	불충분한 식별자, 권한 및 접근관리
	APT (Advanced Persistent Threat)

이처럼, 클라우드 컴퓨팅 환경에서 발생되는 보안 위협은 공유 자원이란 특성에 기인하며 저장된 데이터의 물리적 저장위치를 특정하기 어렵고 데이터가 산재되어 있는 점과 기업의 주요 데이터를 외부환경에 저장함으로 안정성과 신뢰성에 대한 이슈가 주요인으로 파악된다.관련해 주요 위협을 살펴보면 먼저, 클라우드 컴퓨팅의 주요특징인 자원공유가 필연적이고 이를 위해 사용되는 대표되는 가상화 기술과 멀티 테넌시(Multi-Tenancy) 기술의 경우 저장장소와 OS 및 소프트웨어를 공유하는 특징을 가지는데 이런 자원공유에 따른 보안의 경계가 불명확하고 이미지 변조, 가상화 루트킷, VM호핑 등의 가상화 시스템에 대한 직접적인 보안 위협과 보안 경계의 모호함에 따른 중복된 신뢰경계 이슈 등 클라우드 컴퓨팅 환경에 특화된 위협이 발생된다. 또한 기존 On-Premise 환경에서 발생되던 고전적인 네트워크 침해공격, DDoS, 스캐닝, 스니핑, 스누핑 등의 공격이 복합적으로 발생할 수 있다. 이에, 클라우드 컴퓨팅에 대한 보

안 위협에 대응하기 위해 대표적인 클라우드 서비스 제공 기업에서는 클라우드 환경에 적용 가능한 네트워크 보안 및 침입탐지 활동에 필요한 다양한 서비스를 제공하고 있다. 먼저, 아마존에서 제공하는 클라우드 컴퓨팅 서비스로 AWS(Amazon Web Service)가 있으며, AWS는 물리적 보안, 운영체제 보안, 데이터 보안, 어플리케이션 보안에 대한 보안 기능을 제공하고 있으며, 네트워크 보안등 외부에서 공격에 대응하고 클라우드 컴퓨팅 내부 환경 보호를 위해 Web Security Checker, App Security 침입탐지, ACL, 방화벽 등의 보안 기능을 API 형태로 제공하고 있다. Google 또한 클라우드 컴퓨팅 서비스 보호대책으로 DoS 방지, 암호 통신, 사용자 계정, 접근 권한 관리 등의 보안 서비스를 제공하고 있고, 국내 대표 클라우드 서비스 사업자인 KT, Naver 또한 AWS와 유사한 형태의 보안 서비스를 제공하고 있다[2,7].

3. Public 클라우드 통합보안관제 모델

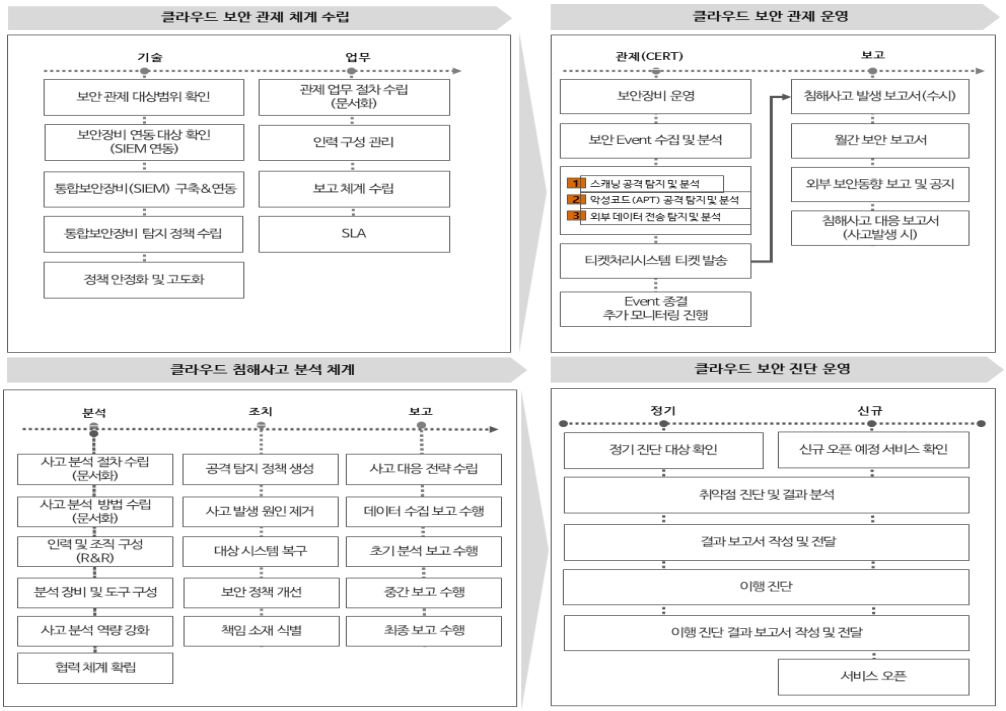
클라우드 컴퓨팅 서비스 환경에서의 보안 위협 증대 및 클라우드 기반 해킹을 통한 중요 정보 유출, 신기술 적용에 따른 보안 취약점 증대와 보안사고 대응 실패 시 기업의 재무적 손실 外 기업 평판에 직접적 타격이 발생할 수 있는 환경이 확산되고 있고, 대외 법규 및 감독 강화, 클라우드 컴퓨팅에 관한 법률, 개인정보보호법 등 관련 Compliance 규제 등에 선제적으로 대응하기 위한 통합적 보안관제 체계가 필요하다. 하지만 기존 클라우드 사업자가 제공하는 보안서비스 적용을 통한 외부 위협 대응 시 기존 기업에서 구축 운영 중인 보안관제 환경과의 상이함에 따른 인력 및 리소스의 중복, On-Premise로 구성된 보안솔루션과의 차이 발생에 따른 관제 활동의 어려움과 On-Premise 보안관제영역과 클라우드 환경의 보안관제 영역이 이분화 되어 비효율적인 보안관제 체계 활동이 야기된다. 또한 국내 컴플라이언스 요건에 충족되지 않은 문제점이 존재한다. 이에 클라우드 서비스 환경 및 보안 위협 변화에 적극 대응하고, 기업별 상이한 보안 정책과 규제를 준수하고 현재 운영 중인 보안관제 체계와 통합할 수 있는 클라우드 통합 보안관제 체계가 필요하다.

3.1 클라우드 통합보안관제 관리체계

클라우드 통합보안관제 체계는 Legacy/Public 클라우드 환경을 고려하여 기존에 구축·운영 중인 On-Premise 네트워크에 대한 보안위협을 대응하기 위해 구성된 DMZ망, 서버망, 사용자망에 구축된 보안관제 시스템을 활용하여 이벤트 모니터링 및 Cert 등의 기존체계는 유지하고 신규로 구축된

〈표 2〉 클라우드 통합 보안관제 관리체계

구분		내용
클라우드 관제 체계	예방	통합 보안 관제 업무 절차 확립 및 사전 예방 훈련 통합 보안 관제 솔루션 구성 및 정책(Rule) 관리 통합 보안관제 분야 각 업무별 담당자 및 인력(R&R) 확립
	탐지	통합 내/외부 위협 탐지 모니터링 정책 통합 이상징후에 대한 오탐 분석 및 사고 식별 업무
클라우드 관제 운영	대응	통합 티켓 시스템을 활용한 침해사고 대응 절차 통합 내/외부 위협에 대한 대응 절차 통합 내부 정보 유출 사고 차단 및 대응 절차
	보고	통합 침해사고 대응 결과에 대한 보고 체계 구성 통합 티켓 시스템을 활용한 침해사고 대응 결과
침해사고 분석체계	분석	통합 침해사고 분석 절차의 적절성 및 명문화 통합 침해사고 조직 및 분석 환경 구성 통합 사고 분석 역량 강화 활동 수행 여부 및 외부 협력 체계
	조치	통합 침해사고 분석에 따른 사고 대응 전략 통합 사고 발생에 대한 책임 소재 식별 기준



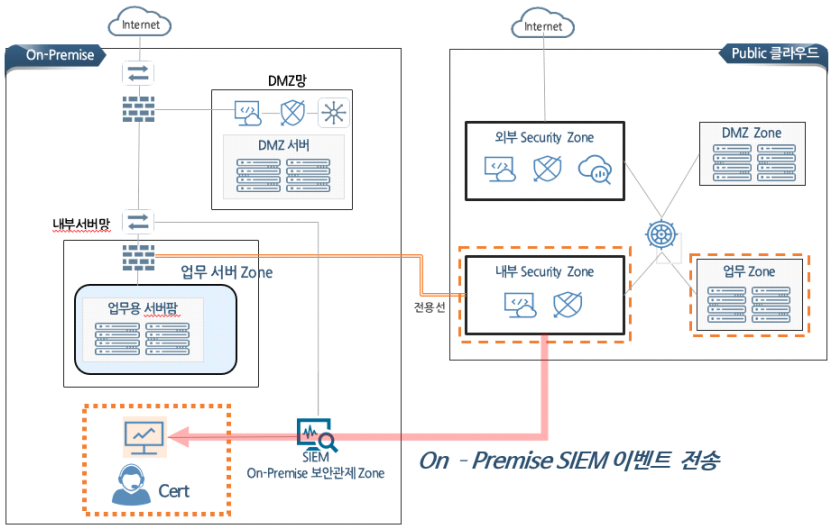
(그림 1) 클라우드 통합 관제 절차

Public 클라우드 컴퓨팅 환경에 대한 내부·외부 접근 통제 및 보안위협에 대응하기 위한 별도의 Security Zone 구성 및 기존 보안관제 환경의 SIEM 시스템에 이벤트 연동을 통한 관제 환경의 변경 없이 동일 수준의 정책 관리와 침해대응 활동을 통해 침해사고 예방 및 대응 활동을 일원화 한다. 이와 함께 클라우드 통합보안관제 관리체계는 예방, 탐지로 구분하여 기존 On-Premise 환경의 보안 관제 업무 절차 확립 및 사전 예방 훈련을 통합하고 각 보안관제 솔루션의 정책(Rule) 관리와 내·외부 위협 탐지 모니터링 정책의 단일화와 이상징후에 대한 오탐 분석 및 사고 식별 업무를 클라우드 서비스 환경에서 동일하게 적용할 수 있게 구성하여 보안관제에 대한 효율성을 높인다. 관련 세부 클라우드 통합 보안관제 관리체계는 <표 2>와 같다.

또한 관제 운영 및 침해사고 분석 체계의 경우 On-Premise 환경에서 내재화된 티켓관리 시스템을 활용한 침해사고 대응 절차, 내/외부 위협에 대한 대응 절차, 내부 정보 유출 사고 차단 및 대응 절차, 침해사고 대응 결과에 대한 보고체계 등의 관리체계를 통합하고 사고 분석 역량 강화 활동 수행 여부 및 외부 협력 체계, 침해사고 분석에 따른 사고 대응 전략, 사고 발생에 대한 책임 소재 식별 기준을 활용하여 신규 클라우드 컴퓨팅 환경에 대한 침해대응 및 분석활동에 대한 추가 자원 및 인력을 최소화 하는 전략을 취한다. 세부 클라우드 보안 관제 절차는 (그림 1)과 같다.

3.2 클라우드 통합 보안관제 아키텍처

클라우드 보안위협 대응을 위해 Cloud Security Zone 을 구성하여 보안위협에 대한 탐지·차단·운영·보고 체계 및 신규 클라우드 서비스 구성 시에도 유연하게 대처 할 수 있는 클라우드 보안 아키



(그림 2) 클라우드 통합 보안관제 환경

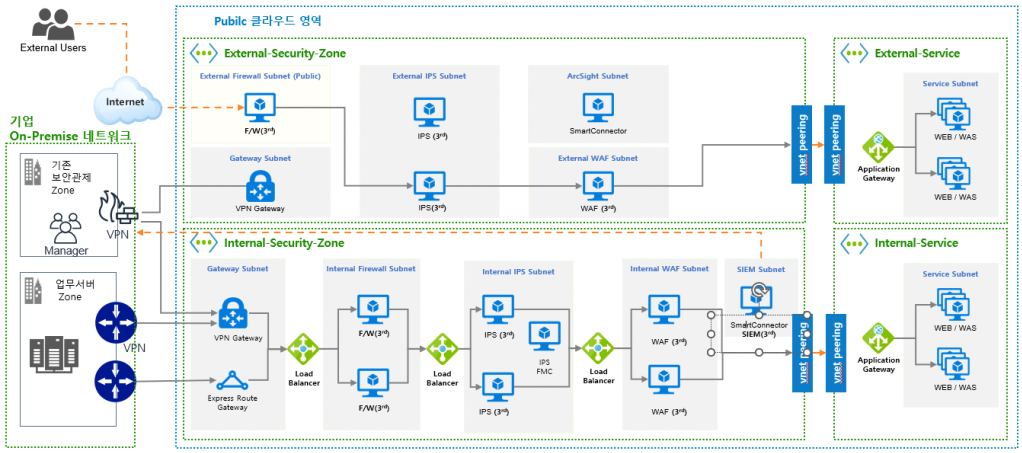
텍처를 구성한다.

먼저, 클라우드 서비스의 구성은 기존 On-Premise 네트워크 환경과 외부 Public 클라우드 환경으로 나누고, 외부 Public 클라우드 환경의 경우 내부 인프라가 구성된 업무 Zone, 외부 서비스 제공을 위한 Public 클라우드 DMZ Zone과 외부와 클라우드 환경이 만나는 접점 구간인 보안솔루션이 설치되는 Security Zone으로 구성한다. 이를 구체적으로 설명하면 기업 On-Premise 내부망 - 클라우드 내부 업무 Zone 구간은 기업 내 사용자 및 클라우드 컴퓨팅을 활용해 구성한 주요 서비스와 연계 및 활용을 위해 연결되는 구간으로 해당 구간을 통해 On-Premise 네트워크 환경에서 사용자나 시스템이 클라우드 컴퓨팅 영역에 직접적으로 연결되며 해당 구간 사이에 내부 Security Zone을 별도 구성하고 트래픽을 거치게 하여 기업 내부망을 통해 확산 되는 위협에 대해 보안통제를 수행한다.

이와 함께 Internet - 클라우드 DMZ Zone 구간은 On-Premise 네트워크 환경에 구성된 DMZ 영역처럼 불특정 외부 사용자의 접근 및 공개된 Web Service를 위한 영역으로 불특정 다수가 접속할 수 있는 해당 구간의 특성 상 보안위협에 대응하기 위한 별도의 외부 Security Zone을 구성하고 유입되는 유해 트래픽을 탐지 및 차단하고, 클라우드 DMZ Zone에서 외부로의 정보유출 및 비인가 접속등에 대한 감시 및 통제를 진행한다.

해당 통합보안관제 아키텍처의 핵심은 각 구간별 경계가 되는 접점에 Security Zone을 별도로 구성하고 네트워크를 통해 유입되는 유해 트래픽을 기존 On-Premise 형태로 구성된 보안관제 환경과 통합하여 보다 효율적인 보안관제 활동을 수행하는데 목적을 둔다. 이처럼 Security Zone에서 발생되는 이벤트를 내부 SIEM으로 전송하여 통합관제를 통해 기업에 운영 중 축적된 Know-How를 기반으로 효과적인 클라우드 컴퓨팅 영역의 보안관제를 수행할 수 있다. 클라우드 보안관제 보안솔루션을 배치하는 방법과 구체적인 클라우드 보안 아키텍처는 (그림 3)과 같다.

클라우드 통합 보안관제 아키텍처를 설계함에 있어 가장 중점을 두어야 할 사항은 첫 째, 침입탐지와 차단에 필요한 FireWall, IPS, WAF 등을



(그림 3) 클라우드 통합 보안관제 아키텍처

3rd Party 보안솔루션으로 구성이 필요하다. 접점 구간인 Security Zone 구성에 필수적인 보안솔루션의 경우 기존 On-Premise 환경에 구축되어 있는 보안솔루션과 동일한 제조사 또는 동등한 수준의 솔루션 구성을 통해 효율적으로 보안관제 활동 수행과 동시에 국내 컴플라이언스 요건에 충족할 수 있게 한다. 둘 째, 클라우드 Security Zone에 구성에 필요한 3rd Party 보안솔루션 도입의 경우 충분한 검증과 TEST가 필요하다. VM 위에 설치 가능한 소프트웨어 방식의 솔루션인지, 클라우드 환경의 특성 상 수시로 변경되는 IP 베이스가 아닌 도메인 기반 통제가능한지, Auto Scaling 등 자원 변화에 유연하게 대응 할 수 있는지 충분히 검증을 통하여 구성하고 관련 탐지 이벤트를 On-Premise 환경에 구축된 SIME으로 전송하여 통합 관제를 수행하여야 한다. 셋 째, 클라 우드 영역 내 각 Zone 간 통신을 위한 연결 방안은 Transit Gateway 구성과 Peering 구성등이 있으며 관리를 용이성 및 트래픽 발생에 따른 비용 등을 고려해 구성한다. 이처럼 기업에서 기존에 운영 중인 보안관제 체계 및 클라우드 환경을 고려한 통합 보안 관제 서비스 수행하고 이를 통해 기존의 보안 정책을 준수하고 보안 위협 분석 및 신속한 대응을 지원할 수 있고 축적된 Know-How를 기반으로 효과적인 클라우드 컴퓨팅 영역의 보안 관제를 수행할 수 있다.

4. 결 론

본 연구에서는 변화하는 비즈니스 환경 대응을 위해 제안되고 있는 클라우드 컴퓨팅 서비스 구축 시 기업 내 운영되고 있는 보안관제 체계와 동등한 보안수준을 만족할 수 있는 클라우드 통합보안 관제 아키텍처에 대해 제안하였다. 먼저, 클라우드 환경에 대한 보안요구 사항을 분석하고, 국·내외 클라우드 서비스에서 제공되는 보안서비스 범위에 대한 분석과 해당 보안서비스에 대한 한계를 밝혔다. 이에 기존 On-Premise 환경에서 구축 운영 중인 보안관제 체계와의 통합 방안으로 관리적 영역의 클라우드 관체체계, 클라우드 관제운영, 클라우드 침해 사고 분석체계에 대한 프로세스 수립 방안과 기술적 영역의 통합보안관제 아키텍처 설계를 위해 기존 On-Premise 네트워크 환경과 외부 Public 클라우드 환경을 나누고 Public 클라우드 환경을 다시 내부 인프라가 구성된 업무 Zone, 외부 서비스 제공을 위한 Public 클라우드

DMZ Zone, 외부와 클라우드 환경이 만나는 접전 구간인 보안관제 영역인 Security Zone 으로 구성되는 3-Tier 구조를 설명하였다. 특히 On-Premise 환경과 클라우드 컴퓨팅 환경의 구간별 경계가 되는 접점에 대한 Security Zone을 별도로 구성하고 네트워크를 통해 유입되는 유해 트래픽을 On-Premise 형태로 구성된 보안관제 환경으로 전달하여 보다 효율적인 보안관제 활동을 수행하여, 기업에 다년간 축적된 보안관제 체계 및 역량을 기반으로 쉽고 빠르며, 비용절감에 효과적인 클라우드 보안관제를 수행할 수 있는 기본 프레임을 제안한 것에 의의가 있다. 이처럼 클라우드 통합보안 아키텍처는 기존 On-Premise 형태의 보안관제 체계를 유지하며, 클라우드 컴퓨팅을 통한 신규서비스 추가로 확장하는 하는 기업에서 활용할 수 있을 것으로 기대한다. 다만, 제안하는 보안관제 아키텍처의 경우 기존 On-Premise 형태의 보안관제 체계를 운영하고 있지 않은 기업에서는 적용성이 떨어지며, 클라우드 컴퓨팅 환경 내부가 업무존 Zone, Security Zone, 클라우드 DMZ 존으로 분리가 되어 있어 각 영역별로 거치는 트래픽에 대한 불필요한 과금이 발생될 수 있다. 향후 연구에서는 관련 문제점을 개선하고 새롭게 개발되는 보안서비스를 지속적으로 검토하여 관련 문제를 개선할 필요가 있다.

참 고 문 헌

[1] DEMPSEY, David; KELLIHER, Felicity. Industry Trends in Cloud Computing. 2018.

[2] VARGHESE, Blesson; BUYYA, Rajkumar. Next generation cloud computing: New trends and researchdirections. Future Generation Computer Systems, pp. 849-861, 2018.

[3] Cloud Security Alliance, “The Treacherous 12 CloudComputing Top Threats in 2016,” Security, no. February, pp.1–34, 2016.

[4] M. Kazim and S. Zhu, “A Survey on Security Threats in CloudComputing Technology,” Int. J. Res., vol. 1, no.8, pp. 1071–1081, 2015.

[5] G. Aswini and R. Mervin, “A Survey on Cloud Security Issuesand Techniques,” Int. J. Comput. Sci. Appl., vol. 4, no. 1, pp.125–132, 2016.

[6] https://cloudsecurityalliance.org/download/top-threats-cloud-computing-plus-industry-insights/

[7] PARK, Jae-Kyung; LEE, Won Joo; LEE, Kang-Ho. A Study on the Isolated Cloud Security Using Next Generation Network. Journal of The Korea Society of Computer and Information, Vol. 22, No. 11, pp. 9-16, 2017.

저 자 약 력

김 영 희

이메일 : younghee22@kopo.ac.kr

- 2018년 서울과학기술대학교 산업정보시스템학과 (박사)
- 2001년~2011년 ㈜인젠 컨설팅본부 팀장
- 2011년~2012년 ㈜인터파크 보안관리팀 개인정보보호 담당
- 2012년~2022년 ㈜한화시스템 보안운영팀 파트장
- 2022년~현재 한국폴리텍대학 사이버보안과 교수
- 관심분야 : 정보보안, 개인정보보안, 정보보안 관리 및 기술체계