情報保護學會論文誌
第 22 卷 第 1 號, 2012. 2

# 통합보안관리시스템을 고려한 IaaS 클라우드 컴퓨팅 운영에 관한 연구

최 주 영†, 박 춘 식‡, 김 명 주
서울여자대학교 정보보호학과

# A Study on Operating the IaaS Cloud Computing in view of Integrated Security Management System

Ju-Young Choi†, Choon-Sik Park‡, Myuhng-Joo Kim
Seoul Women's University Department of Information Security

요 약

클라우드 컴퓨팅 서비스의 표준화 작업을 위해 클라우드 컴퓨팅 서비스에 대한 유즈 케이스와 요구사항 연구가 이루어지고 있지만 클라우드 컴퓨팅 환경의 운영 방법에 대한 연구 자체는 미비하다. 본 논문은 IaaS 클라우드 컴퓨팅 환경의 운영 방법을 기존의 통합보안관리시스템과 연계하여 제안한다. CloudStack 2.2.4 테스트베드를 활용하여 IaaS 클라우드 컴퓨팅 환경을 구축한 SWU-IaaS 클라우드 구조를 먼저 제안한다. 이러한 SWU-IaaS 클라우드 운영을 통해 IaaS 클라우드의 계층적인 구조와 구성요소들에 대한 속성 및 기능을 도출한다. 아울러 IaaS 클라우드 서비스를 정상(normal)적인 상태와 비정상(abnormal)적인 상태로 구분하여 각각의 시나리오를 제시한 후 통합보안관리시스템으로부터 전달되는 보안 이벤트에 대하여 IaaS 클라우드 서비스의 운영 시나리오를 제안한다.

ABSTRACT

In the recent years, various researches on the use cases of the cloud computing service have been achieved for its standardization. Notwithstanding, we need more additory effort to refine the operating mechanisms on the cloud computing environment. In this paper, we suggest an operating mechanism on IaaS cloud computing environment that is related to the integrated security management system. By using CloudStack 2.2.4 toolkit, we have built a test-bed for IaaS cloud computing service i.e., SWU-IaaS cloud computing environment. Through operating this hierarchical SWU-IaaS cloud computing environment, we have derived the attributes and the methods of its components. Its scenarios can be described in case of both normal state and abnormal state. At the end, a special scenario has been described when it receives a security event from the integrated security management system.

**Keywords**: Operating the IaaS Cloud Computing

## I. 서 론

클라우드 컴퓨팅은 IT 컴퓨팅 자원(스토리지, 네트워크 등)을 제3의 특정 영역에 배치한 후 서비스 사용자의 요청에 따라 인터넷 기술을 통해 접근하도록 한 후 사용한 만큼 비용을 지불하도록 하는 서비스 형태

접수일(2011년 12월 27일), 수정일(2012년 2월 15일), 게재확정일(2012년 2월 24일)
† 주저자. jychoi25@gmail.com
‡ 교신저자. csp@swu.ac.kr

이다[1][2][3][4]. 클라우드 컴퓨팅 서비스의 형태는 클라우드 서비스 전달 모델(SaaS, PaaS, IaaS)과 운영 모델(deployment model)의 결합 형태에 따라 다양하게 제공될 수 있으므로 이에 대한 표준화 작업을 위하여 클라우드 컴퓨팅 UCDG(Use Cases Discussion Group)에서는 클라우드 컴퓨팅 유즈케이스를 연구하여 백서[5]를 발표해왔는데 현재 버전은 4.0이다. 참고문헌[5]에서는 유즈케이스 시나리오에 따른 서비스 수준 협약(SLA, Service Level Agreement)과 요구사항을 제시하고 있다. 그러나 유즈케이스 시나리오에서 제공하는 구성요소 간의 요구사항과, 서비스 전달 모델과 운영 모델의 결합에 따른 다양성으로 인하여 클라우드 컴퓨팅 전반에 걸친 운영 모델을 제시하는데 한계가 있다.

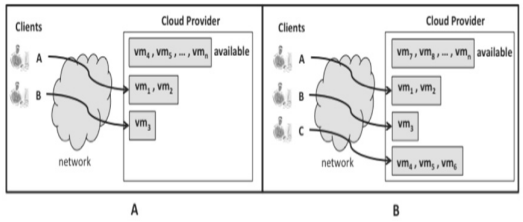
본 논문에서는 클라우드 컴퓨팅 모델 가운데서 IT 컴퓨팅 자원을 서비스 하는 IaaS 클라우드를 연구 범위로 하였다. 선행 연구로 IaaS 클라우드 환경을 제공하는 CloudStack[9] 툴킷을 이용하여 IaaS 클라우드 테스트베드 환경을 구축하였다. 구축한 테스트베드 환경과 NIST 문서 SP800-146[10]에서 제시한 IaaS 클라우드 계층적 컴퓨팅 환경을 바탕으로 SWU-IaaS(Seoul Women's University IaaS) 클라우드를 제안하였다. 제안한 SWU-IaaS 클라우드는 IaaS 클라우드 환경에 기존 통합보안관리시스템[7][8]을 배치하므로 IaaS 클라우드 운영과 함께 통합보안관리시스템으로부터 전달되는 보안 이벤트를 고려한 운영이 요구된다. 본 논문에서는 통합보안관리시스템으로부터 전달된 보안 상태 메시지(normal/abnormal)에 따라 클라우드 서비스 운영 메커니즘이 달라지는 것을 살펴보고 5가지 유형의 시나리오를 통한 검증을 진행하였다.

## II. 관련연구

### 2.1 NIST의 IaaS 클라우드 컴퓨팅 환경

IaaS 클라우드 서비스 제공자는 물리적 자원(스토리지, 네트워킹)을 관리·제공함으로써 IaaS 고객에게 클라우드 인프라 및 환경을 호스팅 한다. IaaS 클라우드 고객은 서비스 수준 협약에 명시된 서비스 범위 안에서 IT 인프라 환경에 대한 서비스를 생성·실행하고 이후의 서비스들에 대하여 관리·모니터링 한다.

NIST는 문서 SP800-146[10]에서 IaaS 클라우드 환경의 동적인 상호작용과 IaaS 클라우드 환경의

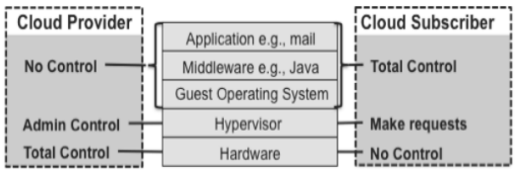



〔그림 1〕 IaaS 제공자와 사용자 간의 동적 상호작용

구성요소의 제어 범위에 대하여 설명하고 있다. 다음 〔그림 1〕은 IaaS 클라우드 환경에서 클라우드 서비스 제공자가 가상머신 자원을 분배하는 상호작용에 대하여 보여주고 있다.

〔그림 1〕의 A는 클라우드 서비스 사용자 A가 VM1과 VM2를 사용하고 클라우드 서비스 사용자 B가 VM3를 사용 중일 때, 클라우드 서비스 제공자는 클라이언트에 제공할 수 있는 가용 VM(Virtual Machine)의 정보(VM4, VM5,…, VMn)를 가지고 있음을 보여준다. 〔그림 1〕의 B는 클라우드 서비스 사용자 C의 요청으로 VM4, VM5, VM6의 자원을 사용할 경우 클라우드 서비스 제공자는 자동적으로 가용 VM 자원에 대한 부가적인 관리가 이루어져야 함을 보여준다. 다음 〔그림 2〕는 IaaS 클라우드 환경의 구성요소인 어플리케이션(application), 미들웨어(middleware), 게스트 Operating System, 하이퍼바이저(hypervisor), 하드웨어(hardware)에 대하여 클라우드 서비스 제공자(Cloud Provider)와 클라우드 고객(Cloud Subscriber)이 각각 제어할 수 있는 범위를 보여준다.

클라우드 서비스 제공자는 물리적 하드웨어에서부터 하이퍼바이저 계층까지를 제어하며, 클라우드 서비스 고객은 게스트 OS에서 상위 계층인 어플리케이션까지를 제어한다. 이러한 IaaS 클라우드 컴퓨팅 환경은 클라우드 서비스 제공자 운영 측면에서 볼 때, 사용자가 요청하는 서비스 항목에 대하여 탄력적으로 서비스를 제공할 수 있어야 하고, 사용자가 언제, 어디서나 접근하여 사용할 수 있도록 서비스의 가용성을




〔그림 2〕 클라우드 구성요소 스택과 제어 범위

보장하는 기술이 필요함을 알 수 있다.

특히 〔그림 2〕에서 살펴본 제어 범위는 보안 사고가 발생했을 때 클라우드 서비스 제공자가 보안적인 측면에서 제어 권한을 갖는 범위라고 볼 수 있으므로 IaaS 클라우드 환경 하에서의 안전한 클라우드 서비스를 위해서는 보안사고 발생에 따른 대응 지침 사항도 서비스 수준 협약에 명시할 필요가 있음을 알 수 있다. 그러나 현재의 클라우드 컴퓨팅 서비스 수준 협약 항목들 가운데 보안과 관련된 요소들은 인스턴스에 대한 모니터링 허용 및 불가, 사고 발생 후 자동 복구 허용 및 불가, 스토리지 가용성 체크, 데이터베이스 가용성 검사 등에 한정되어 있어서 클라우드 서비스 전반에 대한 보안 범위를 다루지 못하고 있다〔11〕.

### 2.2 클라우드 컴퓨팅 환경의 보안 사례

클라우드 컴퓨팅 환경에서 발생한 몇 가지 보안 사고를 살펴보고자 한다. 아마존 EC2 서비스를 제공 받던 일반 사용자가 악의적인 목적으로 소니사의 네트워크를 해킹하여 1억명 이상의 개인 정보를 유출한 사건은 클라우드 서비스가 클라우드 사용자 특히, 해커들에 의해서 충분히 남용될 수 있음을 보여주는 위협적인 사례이다(2011년 5월 15일). 아마존 EC2 서비스 자체의 장애(미러링 과정에서 용량 부족 문제 발생)로 인하여 아마존 서비스와 연계되어 있던 트위터의 클라이언트 홋스위트, 위치정보서비스 포스퀘어, 소셜 질의응답 사이트 쿼라(Quora)등 다수의 서비스와 넷플릭스, 레딧 등 유명 사이트의 서비스가 중단되었던 보안 사고는 클라우드 컴퓨팅 시스템의 관리 분야에서 발생할 수 있는 위협적인 사례이다(2011년 4월 22일). 구글의 이메일 서비스인 Gmail 서비스와 관련하여 이메일 계정 안의 주소록, 폴더, 이용자의 개인 설정, 메일 목록 등 50만명 사용자의 모든 내용이 증발하는 원인 불명의 사고도 발생하여 엔지니어 팀이 모든 이메일을 복구하는 동안 피해를 입은 사용자들은 로그인이 불가능하기도 했다(2011년 2월 28일). 또한 구글 서비스에서 급작스러운 트래픽 증가로 전 세계 Gmail 서비스 사용자의 14% 정보가 서비스 사용에 불편을 겪는 사고가 발생한 바 있다(2009년 5월 16일).

본 연구팀은 지난 연구〔12〕에서 클라우드 서비스 모델(SaaS, PaaS, IaaS)에 따라 클라우드 서비스 제공자의 통합보안관리시스템을 제안하였고 사례별 시나리오를 통해 요구사항 및 해결 방안을 제시한 바 있다. 본 논문에서는 IaaS 클라우드 환경을 제공하는 툴킷인 CloudStack을 테스트베드로 운영하여 구체적인 IaaS 클라우드 서비스 운영 메커니즘을 연구한 후 통합보안관리시스템으로부터 전달되는 보안 상태 메시지에 대하여 IaaS 클라우드 컴퓨팅 환경을 구성하는 컴포넌트들의 유기적인 연동에 관한 연구를 실시하였다.

## III. IaaS 클라우드 컴퓨팅 환경의 테스트베드 운영

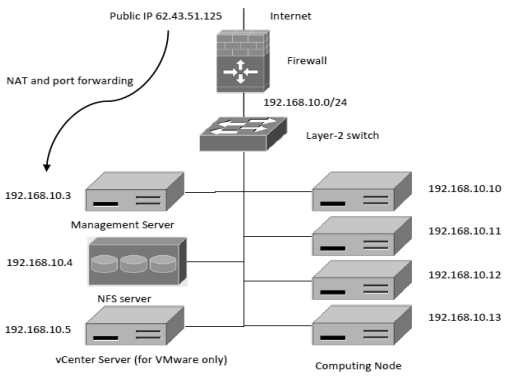
### 3.1 CloudStack 개요

CloudStack은 클라우드 인프라를 형성할 수 있도록 클라우드 서비스 빌드를 제공한다. CloudStack을 활용한 클라우드 서비스 제공자는 서비스 자원에 대한 요구기반(on-demand)의 탄력적인 서비스제공을 지향하므로 클라우드 서비스 사용자에게 빠른 배치와 확장성을 제공할 수 있다. CloudStack 기반 환경을 구축한 클라우드 서비스 제공자는 가상화된 서버를 대응시킬 수 있고 네트워크와 스토리지를 마치 호스팅 공급자처럼 제공할 수 있는 기능을 보유하게 된다. CloudStack은 서비스 및 소프트웨어 패키지를 간단하게 설치할 수 있도록 필수 컴포넌트들을 구축하며 다중 사용(multi-tenant) 기반으로 클라우드 어플리케이션을 관리한다.

### 3.2 CloudStack 구조

CloudStack 2.2.4〔13〕 구조는 IaaS 클라우드 규모와 구성 목적에 따라 다양하게 구축할 수 있다. 일단 물리적 환경의 조건에 따라 논리적인 구성과 서비스가 결정된다. 다음 〔그림 3〕는 소규모의 물리적 조건에 따른 논리적인 구성 사례를 보여준다.

컴퓨팅 노드(Computing Node)들은 지리적으로 분산된 자원으로 각 노드에는 하이퍼바이저가 설치되어 있으며 각 가상머신 위에 게스트 OS를 구성할 수 있다. 게스트 OS와 관련된 컴퓨팅 자원 및 데이터는 논리적으로 일차기억장치(Primary Storage)라는 개념을 적용하여 게스트 가상머신의 루트 디스크 또는 로컬 디스크에 저장된다. 관리서버(Management Server)는 가상머신을 비롯한 클라우드 내의 모든 자원들을 관리한다. 관리콘솔(Management Console)을 제공함으로 관리자가 자원을 직접 제어할 수 있도




〔그림 3〕 CloudStack 구조

록 해준다. 관리서버는 가상머신의 OS를 구성하거나 실행중인 가상머신을 호출할 때 OS 생성 정보에 해당하는 템플릿(template)과 가상머신의 실행 상태인 스냅샷(shapshot)을 이용하게 된다. 이들 정보는 논리적으로 이차기억장치(Secondary Storage)에 저장되고 NFS 서버를 통해서만 접근할 수 있다.

### 3.3 CloudStack 테스트베드 구축 환경

CloudStack 테스트베드 환경은 다음과 같이 구축하였다.

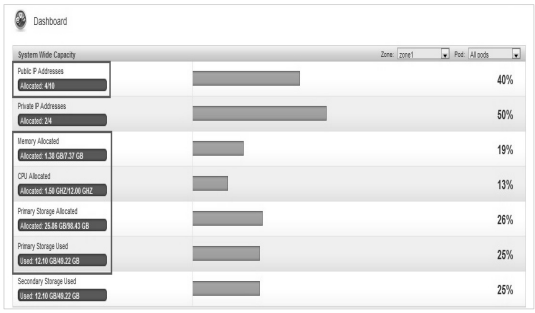
- 관리서버: Fedora 14_x64 - CloudStack
- 하이퍼바이저: Citrix XenServer 5.6 SP2
- NFS 서버: Fedora 14_x64

CloudStack 테스트베드는 다음과 같은 단계로 설치하였다.

- 1단계 : 호스트 구성 - XenServer 설치
- 2단계 : 관리서버 구성
  ① SELinux 및 방화벽 설정 해제 ② 관리서버 설치 ③ 데이터베이스 서버(MySQL DB) 설치
- 3단계 : NFS 서버 구성
  ① NFS 서버 설정 ② 기억장치 셋업
- 4단계 : 논리적 환경 구성 (Zone → 클러스터 → 호스트→ 일차기억장치 → 이차기억장치)

### 3.4 CloudStack 테스트베드 운영

CloudStack는 템플릿을 선택하여 게스트 가상머신을 추가할 수 있으며 사용자 임의 템플릿을 추가하여 인스턴스를 생성할 수 있다. 이러한 방법을 통하여




〔그림 4〕 CloudStack - Dashboard 화면

생성된 정보는 다음 〔그림 4〕와 같이 계기판(dashboard)을 통해 자원 할당 정보와 상태를 확인할 수 있다.

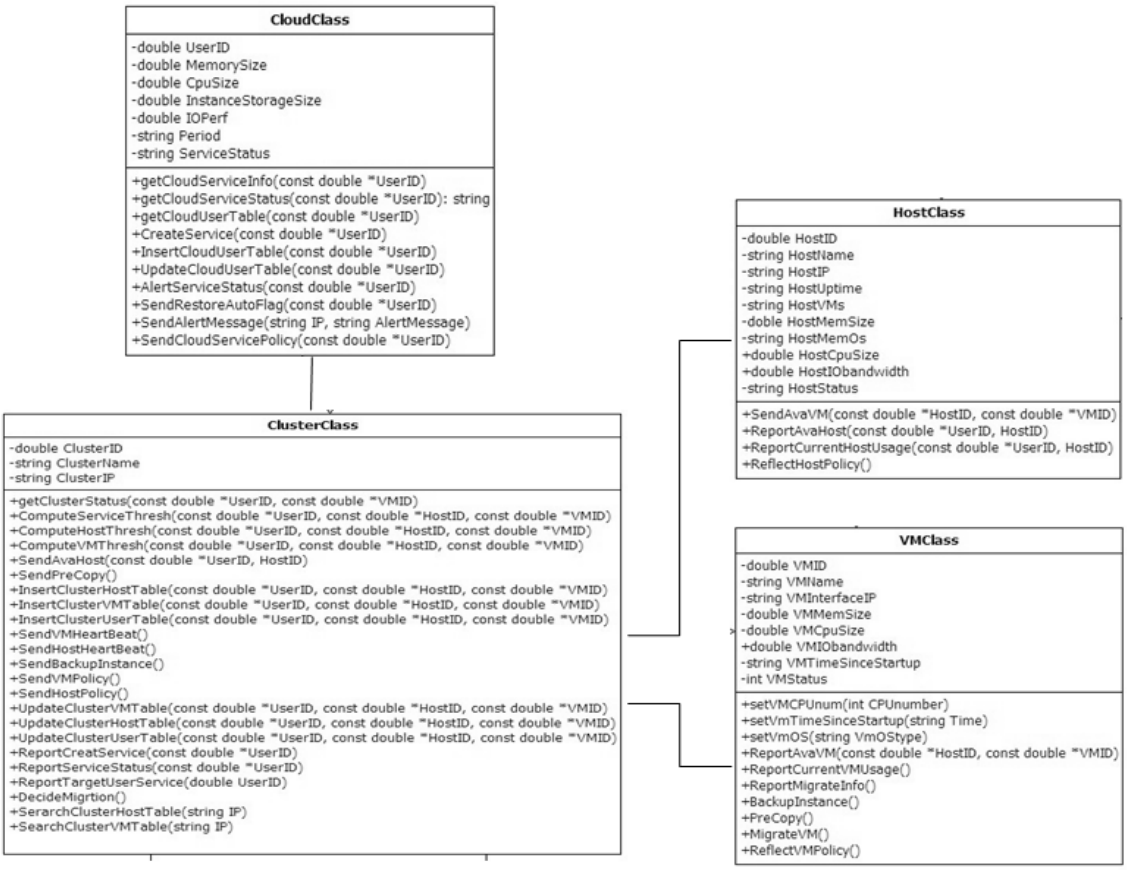
CloudStack은 설치 및 환경 구성하는 과정에서 발생한 문제에 대한 로그 정보를 management-server.log 파일에서 확인할 수 있다. 예를 들어, 이차기억장치 가상머신 접근에 문제가 발생할 경우 진단 스크립트(diagnostic script)를 실행하거나 로그 파일을 확인하여 문제를 해결할 수 있다. 콘솔뷰어(ConsoleViewer)에 접근하지 못한다거나 "Access is denied for console session" 라는 메시지가 발생하는 문제는 Console Proxy VM이 개별 인터페이스에서 관리서버(또는 부하균형이 이루어지는 관리서버 풀)의 8250 포트에 제대로 접근하지 못한다는 것을 의미하는 것으로, 부하 균형모듈의 8250포트와 관리서버의 8250포트 등 해당 포트에 대한 사용 여부를 확인하거나 호스트의 글로벌 설정 값을 확인함으로써 발생한 문제를 해결한다.

CloudStack 테스트베드를 설치·운영과 함께 NIST 문서 SP800-146〔10〕에서 제시한 IaaS 컴퓨팅 구조를 토대로 IaaS 클라우드 컴퓨팅 환경의 구성요소(Cloud Manager, Cluster Manager, Computer Manager(Host, VM))을 모델링하여 각 구성요소의 속성 및 기능에 대하여 다음 〔그림 5〕와 같이 도출하였다.

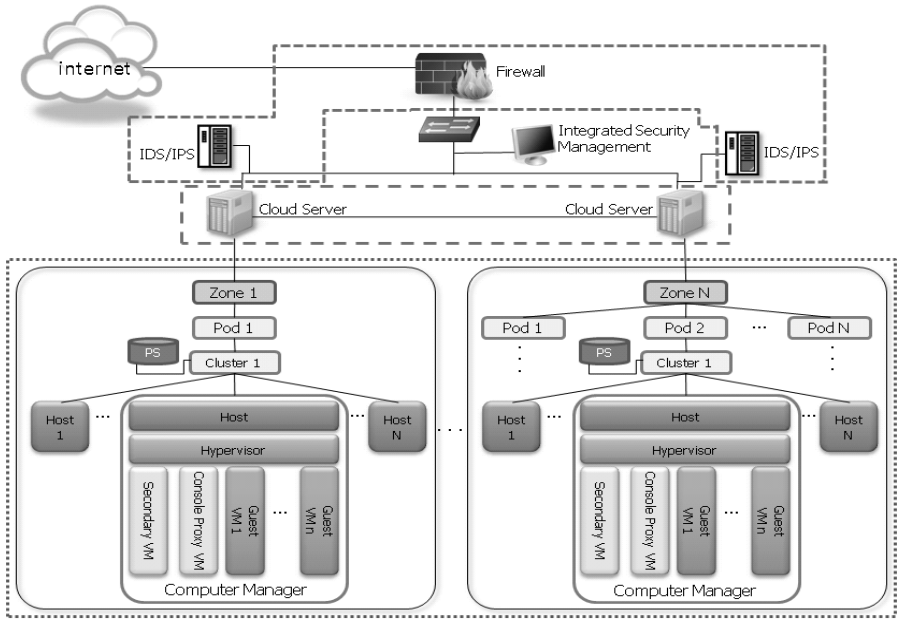
## IV. 통합보안관리시스템 연동을 위한 SWU-IaaS 클라우드 운영 제안

### 4.1 제안한 SWU-IaaS 클라우드 구성

SWU-IaaS 클라우드 구조는 다음 〔그림 6〕와 같다. 클라우드 서버(Cloud Server)는 가상화 환경을




〔그림 5〕 SWU-IaaS 클라우드의 객체 모델링




〔그림 6〕 SWU-IaaS 클라우드 구성도

구성한 후 이를 운영한다. [그림 6]의 구성요소는 다음과 같다.

- ○ 클라우드 서버(Cloud Server) 또는 클라우드 관리자(Cloud Manager) : CloudStack 설치
- ○ 호스트(Host) : 할당된 게스트 VM의 CPU와 메모리 자원 제공
- ○ 일차기억장치(PS, Primary Storage) : 게스트 VM의 루트 디스크 저장
- ○ 이차기억장치(Secondary Storage) : 템플릿과 스냅샷 저장

클라우드 서비스는 사용자 요청에 의해 이차기억장치(Secondary Storage)에 있는 템플릿을 이용하여 Zone → Pod → Cluster 순서로 가상화 환경을 구성한다. 클러스터(Cluster)는 일차기억장치(PS, Primary Storage)와 Host를 추가하여 Dom0 영역에 Secondary VM, Console Proxy VM을 생성하고 이후 게스트 VM를 생성하여 클라우드 서비스 환경을 제공한다.

SWU-IaaS는 IaaS 클라우드 환경과 통합보안관리시스템(예, 방화벽, IDS, IPS 등)이 함께 구성된 것으로 서비스 가용성 보장을 위한 SWU-IaaS 클라우드 운영에 통합보안관리시스템으로부터 전달되는 메시지를 고려할 필요가 있다. 본 연구에서는 전달되는 보안 상태 메시지를 정상적인 상태(normal)와 비정상적인 상태(abnormal)로 나누었다. 정상적인 상태는 통합보안관리시스템으로부터 보안 이벤트 정보가 전달되지 않았을 때를 의미하고, 비정상적인 상태은 보안 이벤트 정보가 전달되었을 때를 의미한다.

다음은 SWU-IaaS 클라우드 운영 절차에 보안 상태 메시지를 접목한 메커니즘을 제안하고 시나리오를 적용하여 검증하도록 한다.

### 4.2 SWU-IaaS 클라우드 운영 시나리오

SWU-IaaS 클라우드 운영 시나리오는 [그림 6]의 구성요소인 클라우드 서버, 클러스터, 호스트, 가상머신(VM)간의 처리과정에 대하여 순차다이어그램을 이용하여 설명한다. 본 논문에서는 SWU-IaaS 클라우드의 서비스 가용성 보장 관점으로 연구 범위를 제한하였다. 시나리오는 통합보안관리시스템으로 전달되는 보안 상태 메시지(normal/abnormal)정보를 기준으로 클라우드 서비스 시작에서부터 가상 자원을 운영하는 과정에 대한 5가지 유형을 다음과 제시하였다.

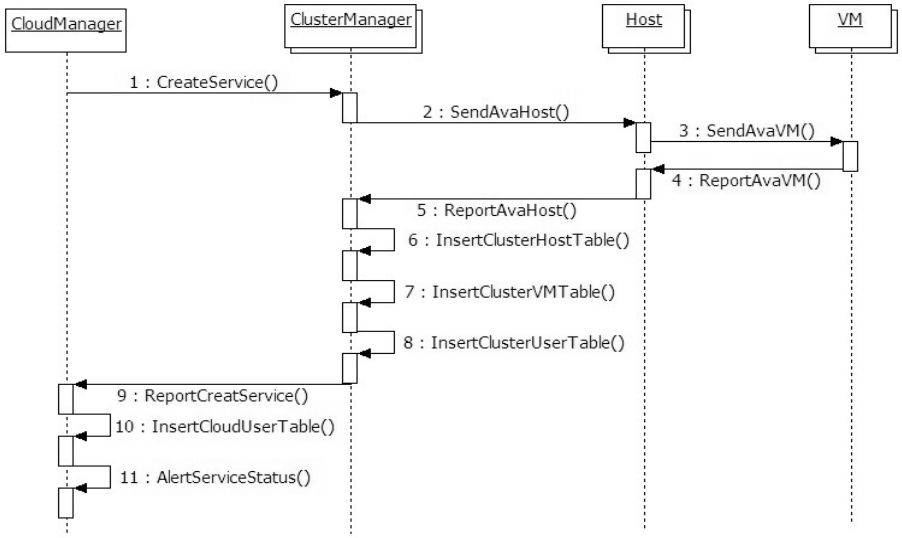
- ○ 시나리오 1 : (normal) SWU-IaaS 클라우드 서비스 요청
- ○ 시나리오 2 : (normal) SWU-IaaS 클라우드 서비스 운영
- ○ 시나리오 3 : (normal) 서비스 사용자의 사용량 초과
- ○ 시나리오 4 : (normal) 가상머신의 임계값 초과
- ○ 시나리오 5 : (abnormal) 통합보안관리시스템으로부터 보안 이벤트 메시지 도착

#### 4.2.1 시나리오 1 : (normal) SWU-IaaS 클라우드 서비스 요청

사용자의 요청으로 SWU-IaaS 클라우드 서비스를 시작할 때 클라우드 제공자는 사용자 요청을 수행할 수 있는 가상화 환경이 가능한지에 대한 여부를 먼저 확인해야 한다. 이에 대하여 클러스터 관리자(Cluster Manager)는 호스트와 가상머신에게 사용자 요청 규모에 적합하면서도 사용 가능한 호스트와 가상머신을 적용할 수 있는지 확인하는 절차를 갖는다. 시나리오 1에 대한 요구사항을 다음과 같이 정리하였다.

- ○ 클라우드 관리자(Cloud Manager)는 클라우드 서비스 사용자와 접근 포인터 역할을 함
- ○ 서비스 사용자와 클라우드 관리자는 사용할 서비스 항목과 서비스 수준 협약 항목에 대하여 체결함
- ○ 사용자의 서비스 개시 요청이 발생하면 서비스 항목(CPUnumber, CPUspeed, MemorySize, InstanceStorageSize등)에 해당하는 사용 가능한 가상 자원 확보 여부 확인함
- ○ 클라우드 관리자는 클러스터 관리자(Cluster Manager)로부터 서비스 자원 확보 가능 여부 메시지에 따라 사용자와 서비스 체결 절차 진행함
- ○ 클라우드 관리자는 사용자의 서비스 정보 테이블을 가지고, 클러스터 관리자는 호스트, 가상머신, 사용자의 서비스 정보에 대한 각 테이블을 가짐

다음은 위에서 명시한 시나리오 1에 대한 요구사항




〔그림 7〕 시나리오 1 : SWU-IaaS 클라우드 서비스 요청 순차다이어그램

〔표 1〕 시나리오 1 단계 설명

| 단계 | 설 명 |
|---|---|
| 1 | 서비스 사용자의 요청 정보 Cluster Manager에게 전달함 |
| 2~3 | 사용 가능한 Host와 VM 정보를 요청함 |
| 4~5 | 사용 가능한 Host와 VM 정보를 전달함 |
| 6~8 | Cluster Manager의 테이블(ClusterHost-Table, ClusterVMTable, ClusterUserTable)에 사용자 정보를 포함한 데이터를 추가함 |
| 9 | 생성된 서비스 환경 정보를 Cloud Manager에게 전달함 |
| 10 | Cloud Manager의 테이블(CloudUserTable)에 사용자 정보의 데이터를 추가함 |
| 11 | 서비스 사용자에게 서비스 상태 정보를 전달함 |

을 반영한 SWU-IaaS 클라우드 서비스 요청 순차다이어그램〔그림 7〕 및 설명〔표 1〕이다.

### 4.2.2 시나리오 2 : (normal) SWU-IaaS 클라우드 서비스 운영

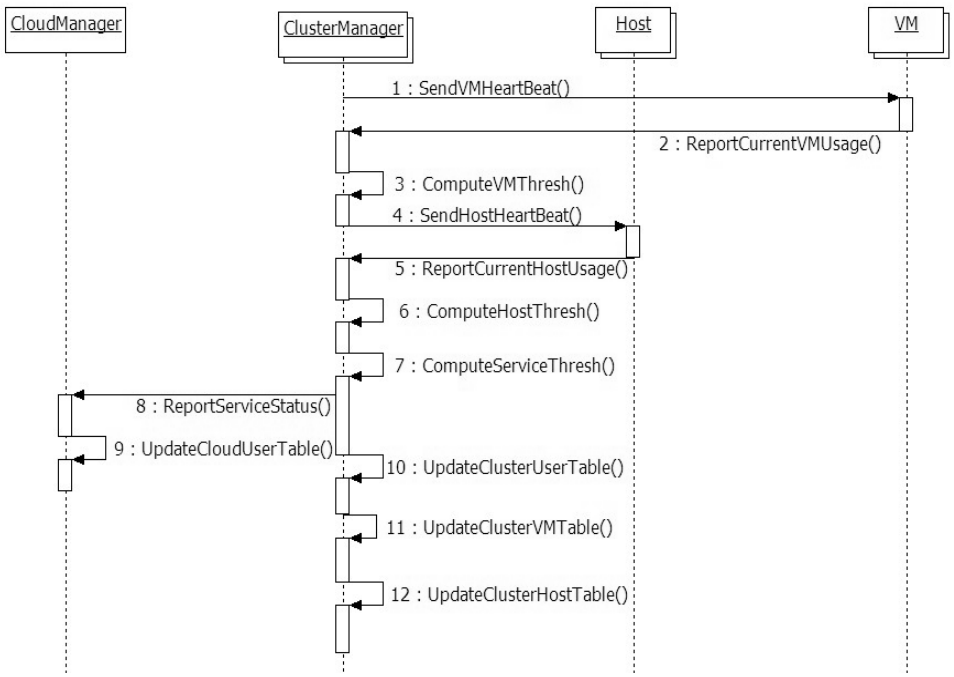
SWU-IaaS 클라우드 모델은 주기적으로 가상화 환경의 현재 상태를 리포팅 받아서 클라우드 서비스 사용자의 안정성을 보장해야한다. 이를 위해 클러스터 관리자는 호스트와 가상머신에게 HeartBeat 신호를 전달하여 호스트와 가상머신의 현재 사용률 값을 전달

〔표 2〕 시나리오 2 단계 설명

| 단계 | 설 명 |
|---|---|
| 1~3 | Cluster Manager는 VM에게 HeartBeat 신호를 전달하여 현재의 사용률을 전달 받는다. 전달된 VM 사용률 값은 VM의 크기와 한계점(Limit)을 기준으로 VM의 임계값을 도출함 |
| 4~6 | Host에게 HeartBeat 신호를 전달하여 현재의 사용률을 전달 받는다. 전달된 Host 사용률 값은 Host의 크기와 한계점(Limit)을 기준으로 Host의 임계값을 도출함 |
| 7 | 1~6 단계의 과정을 통해 서비스 사용자의 자원(메모리, CPU, I/O)에 대한 임계값을 도출함 |
| 8 | Cloud Manager에게 서비스 사용자의 자원에 대한 상태 정보를 전달함 |
| 9 | 변경된 정보가 있을 경우 Cloud Manager의 테이블(CloudUserTable)을 업데이트함 |
| 10~12 | Cluster Manager의 테이블(ClusterUser-Table, ClusterHostTable, ClusterVMTable)을 업데이트함 |

받는다. 시나리오 2에 대한 요구사항을 다음과 같이 정리하였다.

- ○ 클러스터 관리자는 해당 클러스터 영역에 존재하는 호스트와 가상머신에 대하여 주기적으로 상태 확인 필요함
- ○ 주기적인 확인 메시지를 전달받은 호스트와 가상머신은 클러스터 관리자에게 사용량 정보를 전달함




〔그림 8〕 시나리오 2 : SWU-IaaS 클라우드 서비스 운영 순차다이어그램

○ 클러스터 관리자는 전달된 호스트와 가상머신 정보를 사용자 서비스 단위로 계산하여 클라우드 관리자에게 서비스 상태 정보로 전달함

시나리오 2에 대한 요구사항을 반영한 SWU-IaaS 클라우드 서비스 운영 순차다이어그램〔그림 8〕 및 설명〔표 2〕이다.

#### 4.2.3 시나리오 3 : (normal) 서비스 사용자의 사용량 초과

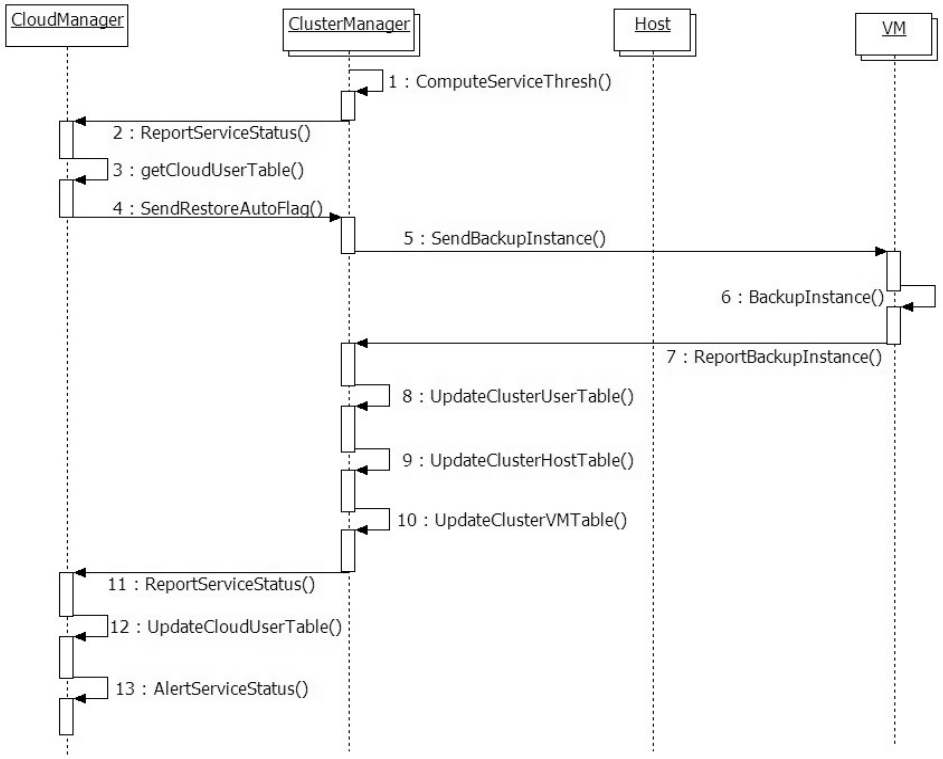
SWU-IaaS 클라우드 서비스 운영 과정에서 사용자가 요청한 자원보다 사용량이 초과되었을 때 이에 대한 처리 과정을 시나리오 3에서 설명한다. 시나리오 3에 대한 요구사항을 다음과 같이 정리하였다.

○ 시나리오 2의 단계 7에서 서비스 사용자의 사용량이 초과했을 때 이에 대한 처리 과정 필요함
○ 클라우드 관리자는 시나리오 1의 서비스 체결 시 설정한 서비스 수준 협약 항목 가운데 자동 백업 플래그(ResotreAutoFlag)를 확인하여 인스턴스 정보의 백업 진행 여부 결정함
○ 백업 진행 이후 서비스 상태 정보를 사용자에게 전달함

시나리오 3에 대한 요구사항을 반영한 서비스 사용자의 사용량 초과 순차다이어그램〔그림 9〕 및 설명〔표 3〕이다.

〔표 3〕 시나리오 3 단계 설명

| 단계 | 설 명 |
|---|---|
| 1~2 | Cluster Manager에서 서비스 사용자의 임계값을 도출하는 과정에서 사용량 초과가 발생하여 Cloud Manager에게 서비스 사용자 상태 정보를 전달함 |
| 3 | Cloud Manager는 CloudUsertTable에서 인스턴스 내에 문제가 발생했을 때 복구를 위한 백업 실시 여부에 대한 정보를 가져옴. 백업 실시 허용을 선택했을 경우 Cluster Manager에게 백업 진행을 위해 4단계로 실행함. 백업 실시 불가를 선택했을 경우, 제공되는 서비스를 중지하는 절차를 진행함 |
| 4~7 | Cluster Manager에게 백업 진행을 VM에게 전달하여 백업을 실시함. 백업 진행 과정에 대한 결과를 Cluster Manager에게 전달함 |
| 8~11 | Cluster Manager는 사용량 초과로 발생한 백업 정보를 ClusterUserTable의 Instance-Backup에 저장함. 백업으로 변경된 Host와 VM 정보를 각 테이블(ClusterHostTable, ClusterVMTable)에 갱신함. 변경된 서비스 사용자 정보를 Cloud Manager에게 전달함 |
| 12~13 | Cloud Manager의 CloudUserTable을 갱신함. 사용자에게 서비스 상태 정보를 전달함 |




〔그림 9〕 시나리오 3 : 서비스 사용자의 사용량 초과 순차다이어그램

#### 4.2.4 시나리오 4 : (normal) 가상머신의 임계값 초과

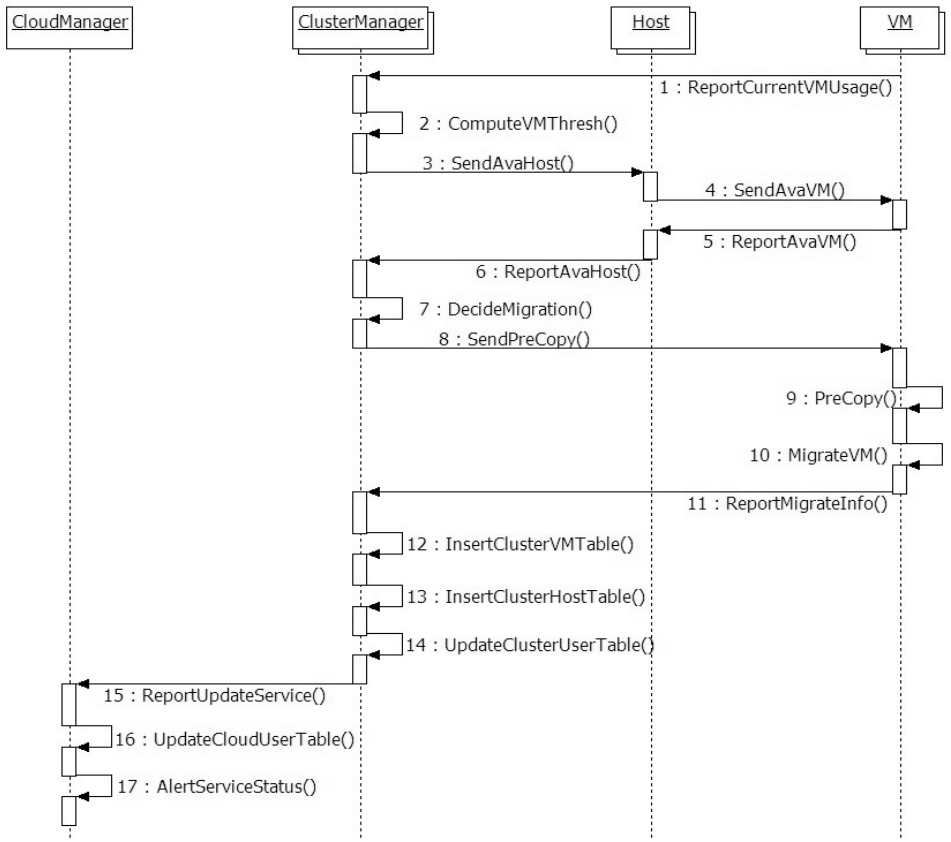
SWU-IaaS 클라우드는 가상화〔14〕〔15〕〔16〕〔17〕 환경을 기반으로 가상 자원을 사용자에게 서비스한다. 따라서 서비스의 가용성 보장을 위하여 시나리오 2에서 주기적으로 가상 자원을 구성하는 호스트와 가상머신의 상태 정보를 확인하였다. 시나리오 4는 시나리오 2의 주기적인 상태 확인 과정에서 가상머신의 임계값이 초과한 상태에 대한 문제 해결에 대한 시나리오이다. 이에 대한 요구사항은 다음과 같다.

- ○ 시나리오 2의 단계 3에서 가상머신의 임계값 초과 상태인 경우 마이그레이션〔18〕〔19〕〔20〕이 필요함
- ○ 클러스터 관리자는 가상머신의 마이그레이션을 위해 사용 가능한 가상머신 선정 과정 필요함
- ○ 마이그레이션 과정으로 변경된 사용자의 서비스 정보를 클라우드 관리자에게 전달함

시나리오 4에 대한 요구사항을 반영한 가상머신의 임계값 초과 순차다이어그램〔그림 10〕 및 설명〔표 4〕이다.

〔표 4〕 시나리오 4 단계 설명

| 단계 | 설 명 |
|---|---|
| 1~4 | Cluster Manager는 주기적으로 VM의 상태를 모니터링하고 VM의 임계값을 계산함. 이 과정에서 VM의 임계값이 초과될 경우 먼저 대체 가능한 Host와 VM을 찾음 |
| 5~7 | 대체 가능한 Host와 VM 정보를 전달 받아 마이그레이션 작업 수행을 결정하게 됨. 이때 Cluster Manager에서 마이그레이션 대상 가상머신 선정 정책에 따라 결정됨 |
| 8~11 | 마이그레이션 대상 정보과 목적 정보를 가지고 precopy 진행을 실시한 후 마이그레이션 작업을 수행함. 마이그레이션 작업 완료 후 Cluster Manager에게 결과 정보를 전달함 |
| 12~15 | Cluster Manager는 ClusterUserTable의 HostID, VMID등 변경된 정보를 갱신하고 ClusterHostTable과 ClusterVMTable의 추가 및 변경된 정보를 레코드에 추가하고 갱신을 진행함. 변경된 서비스 사용자의 상태 정보를 Cloud Manager에게 전달함 |
| 16~17 | 변경된 서비스 사용자 정보를 CloudUserTable에 갱신한 후 사용자에게 서비스 상태 정보를 전달함 |




〔그림 10〕 시나리오 4 : 가상머신의 임계값 초과 순차다이어그램

#### 4.2.5 시나리오 5 : (abnormal) 통합보안관리시스템으로부터 보안 이벤트 메시지 도착

SWU-IaaS 클라우드 구조는 IaaS 클라우드 환경에 기존 통합보안관리시스템을 배치함으로 IaaS 클라우드 운영 시 통합보안관리시스템으로부터 전달되는 보안 이벤트 정보에 대한 처리 과정이 필요하다. 예를 들어 특정 가상머신 자원(스토리지, CPU 등)에 과부하가 발생한 경우, 앞에서 살펴본 시나리오 2의 3단계(ComputeVMThresh), 6단계(ComputeHost-Thresh), 7단계(ComputeServiceThresh) 과정에서 문제가 발견되어 시나리오 3과 시나리오 4의 과정을 통해 해결될 수 있다. 그러나 이것은 보안 상태 메시지가 정상적일 때 가능한 처리 과정이다. 보안 상태 메시지가 비정상적인 경우 클라우드 관리자는 SWU-IaaS 클라우드 환경을 유지하기 위하여 문제의 가상머신 자원에 보안 정책을 반영할 필요성이 있다. 시나리오 5는 비정상적인 상태(abnormal)로 통합보안관리시스템으로부터 특정 가상머신의 문제 발

〔표 5〕 시나리오 5 단계 설명

| 단계 | 설 명 |
|---|---|
| 1~4 | Cloud Manager가 기존 관제시스템으로부터 서비스 거부 공격 메시지(IP addr, Alert_level, Service Name등)를 전달 받으면 서비스 거부 공격 대상의 Host와 VM 정보를 얻기 위해 Cluster Manager에게 Host와 VM 정보를 요청한다. Cluster Manager는 공격 대상 서비스 사용자 정보를 Cloud Manager에게 전달함 |
| 5~14 | 서비스 사용자와 서비스 체결 당시 결정된 서비스 수준 협약을 기준으로 하여 클라우드 환경 보안 정책을 결정한 후 이를 Cluster Manager에게 전달함. Cluster Manager는 VM →Host 순서로 클라우드 보안 정책을 반영함. 정책에 반영된 VM과 Host는 해당 처리 결과를 Cluster Manager에게 보고함. 보안 정책 반영으로 변경된 정보는 각 테이블 ClusterVMTable, ClusterHostTable, ClusterVMTable에 갱신됨 |
| 15~17 | Cluster Manager로부터 보안 정책이 반영된 결과를 전달 받은 Cloud Manager는 변경된 정보를 바탕으로 CloudUserTable를 갱신한 후 사용자에게 서비스 상태 정보를 전달함 |


〔그림 11〕 시나리오 5 : 통합보안관리시스템으로부터 보안 이벤트 메시지 도착 순차다이어그램

생에 대한 메시지를 전달 받았을 때 처리 과정을 설명한다. 시나리오 5에 대한 요구사항을 다음과 같이 정리하였다.

- ○ 클라우드 관리자는 전달 받은 문제의 가상머신에 대한 정보 확인 필요함
- ○ 클라우드 관리자는 해당 가상머신 사용자의 서비스 수준 협약 항목과 보안사고 범위(SWU-IaaS 클라우드 서비스 전체/일부)를 결정함
- ○ 클라우드 관리자는 보안 정책을 해당 문제의 가상머신에 적용함

시나리오 5에 대한 요구사항을 반영한 통합보안관리시스템으로부터 보안 이벤트 메시지 도착에 대한 순차다이어그램〔그림 11〕 및 설명〔표 5〕이다.

## V. 결 론

클라우드 컴퓨팅은 IT 자원을 언제 어디서나 서비스 사용자의 요구 정보에 탄력적으로 대응할 수 있도록 하기 위하여 가상화 기술을 기반으로 자동화된 프로비져닝 기술을 제공한다. 클라우드 서비스는 서비스 전달 모델과 운영 모델을 기준으로 서비스 유형을 정리할 수 있으며 이들 모델의 결합에 의하여 다양한 형태의 서비스들이 제공된다. 일반적으로 표준화 연구를 위하여 다양한 클라우드 서비스에 대한 유즈케이스와 그에 대한 요구사항이 연구되고 있다.

본 논문에서는 IaaS 클라우드 컴퓨팅 환경에 특정하여, 기존 통합보안관리시스템을 배치한 IaaS 클라우드 환경을 구성하였다. 이를 위해 앞서 IaaS 클라우드 환경을 구축하는 툴킷인 CloudStack 2.2.4을 이용하여 IaaS 클라우드 테스트베드를 구축하였다. 이처럼 구축한 IaaS 클라우드 테스트베드와 NIST에서 제시한 IaaS 클라우드 구조를 토대로 본 논문에서는 SWU-IaaS 클라우드 구조를 제안한 후 SWU-IaaS 클라우드의 계층적 구조를 갖는 구성요소에 대한 속성 및 기능을 도출하였다. 아울러 SWU-IaaS 클라우드 환경 하에서 기존 통합보안관리시스템을 배치하여 통합보안관리시스템으로부터 보안 상태 메시지를 정상(normal)적인 상태와 비정상(abnormal)적인 상태로 구분한 후, 클라우드 서비스의 정상적인 상태로는 서비스 시작과 운영 시나리오에 적용하였고 비정상적인 상태로는 통합보안관리시스템으로부터 전달되는 보안 이벤트 메시지 처리 절차에 대한 시나리오를 제시하였다.

본 연구에서 제시한 IaaS 클라우드 컴퓨팅 운영에 대한 시나리오는 클라우드 서비스 제공자 측면에서는 서비스 운영에 대한 핵심적인 참고자료로 활용될 수 있으며 클라우드 서비스 사용자 측면에서는 IaaS 클라우드 컴퓨팅 운영에 대한 총체적인 이해를 도울 것이다. IaaS 클라우드 컴퓨팅 환경에서 클러스터 관리자(Cluster Manager) 계층의 운영과 보안 관리의 집중화로 인하여 병목현상이 발생하는 경우 이를 해결할 수 있는 알고리즘에 대한 연구가 앞으로 이루어질 것이다.

## 참고문헌


〔1〕 P.Mell and T.Grance, "The NIST Definition of Cloud Computing, National Institute of Standards and Technology", National Institute of Standards and Technology, ver.15,9 pp. 1-2, July 2010.

〔2〕 Gartner, "Gartner Highlights Five Attributes of Cloud Computing", Available at: http://www.gartner.com/it/page.jsp?id=103501

〔3〕 박원환, "정보통합전산센터 스토리지 가상화 구축 사례", 클라우드 컴퓨팅과 스토리지 가상화 콘퍼런스 발표집, pp. 2-4, 2009년 9월.

〔4〕 ENISA, "Cloud Computing: Benefits, risks and recommendations for information security", European Network and Information Security Agency, pp. 14-16 , Nov. 2009.

〔5〕 Cloud Computing Use Cases Discussion Group, "Cloud Computing Use Cases White Paper", Version 4.0, 2 pp. 18-61 ,July 2010.

〔6〕 Michael Hogan, Fang Liu, Annie Sokol and Jin Tong, "NIST Cloud Computing Standards Roadmap", National Institute of Standards and Technology, SP 500-291, pp. 14-30, July 2011.

〔7〕 Renaud Bidou, "Security Operation Center Concepts & Implementation", Available at:http://www.iv2-technologies.com/SOCConceptAndImplementation.pdf

〔8〕 "정보보호시스템간 통합보안관리 시스템 개발", 정보통신부, pp. 21-30, 2001년 11월.

〔9〕 CloudStack. Available at: http://cloudstack.org/cloudstack.html

〔10〕 Lee Badger, Tim Grance, Robert Patt-Corner and Jeff Voas, "DRAFT Cloud Computing Synopsis and Recommendations", National Institute of Standards and Technology, SP800-146, pp. 7-1 - 7-8 ,May 2011.

〔11〕 Radhesh Balakrishnan, "Delivering IT as a Service", Cloud&Data center 2011, Microsoft, pp. 5-6, April 2011.

〔12〕 Ju-Young Choi, Hyung-Jong Kim, Choon-Sik Park and Myuhng-Joo Kim, "Integrated Security Management against the Weakness of Virtualization in Cloud Computing", The 4th International Conference on Convergence Technology and Information Convergence, pp. 17-23, July 2009.

〔13〕 Cloud.com, "Cloud.com CloudStack Installation Guide", Version 2.2.4-2.2.7, pp. 11-16, June 2011.

〔14〕 Karen Scarfone, Murugiah Souppaya and Paul Hoffman, "Guide to Security for Full Virtualization Technologies", National Institute of Standards and Technology,SP 800-125, pp. 2-1 - 2-8 ,January 2011.

〔15〕 Catbird Networks, "Virtualization Security : The Catbird Primer", pp. 3, September 2008.

〔16〕 이효, "가상화 기반의 클라우드 컴퓨팅", 한국정보보호학회 클라우드컴퓨팅연구회, pp. 4-14, 2009년 5월.

〔17〕 Citrix Systems, "Xen Architecture Overview", pp. 3-8, February 2008.

〔18〕 Christopher Clark, Keir Fraser, Steven Hand and Jakob Gorm Hanse, "Live Migration of Virtual Machines", NSDI'05 Proceedings of the 2nd conference on Symposium on Networked Systems Design & Implementation - Volume 2, NSDI USENIX Symposium, pp. 1-10, Jun

2005.
〔19〕 F. Hao, "Enhancing Dynamic Cloud-based Services using Network Virtualization", ACM VISA, pp. 37-44, August 2009.
〔20〕 J. Oberheide, "Empirical Exploitation of Live Virtual Machine Migration", Black-Hat Symposium, pp. 1-6, March 2008.

## 〈著者紹介〉

최 주 영 (Ju-Young Choi) 정회원
1999년: 서울여자대학교 컴퓨터학과 이학사
2003년: 서울여자대학교 컴퓨터학과 이학석사
2012년: 서울여자대학교 컴퓨터학과 이학박사
〈관심분야〉 클라우드컴퓨팅보안, 정보보안

박 춘 식 (Choon-Sik Park) 종신회원
1995년: 일본동경공업대 공학박사
1982년~1999년: 한국전자통신연구원 책임연구원
2000년~2008년: 국가보안기술연구소 책임연구원
2009년 3월~현재: 서울여자대학교 정보보호학과 교수
〈관심분야〉 개인정보보호기술, 클라우드컴퓨팅보안

김 명 주 (Myuhng-Joo Kim) 종신회원
1986년 2월: 서울대학교 컴퓨터공학과 공학사
1988년 2월: 서울대학교 컴퓨터공학과 공학석사
1993년 8월: 서울대학교 컴퓨터공학과 공학박사
1993년 9월~1995년 8월: 서울대학교 컴퓨터 신기술 공동연구소 특별연구원
2003년, 2010년: 미국 펜실베이니아대학교(UPenn) 객원 연구원
1995년~현재: 서울여자대학교 정보보호학과 교수
〈관심분야〉 소프트웨어보안, 악성코드, 웹보안, 창의성과 윤리