http://dx.doi.org/10.14400/JDC.2014.12.11.299

클라우드 데이터센터로의 전환을 위한 보안요건 - N데이터센터를 중심으로

나종회*, 이재숙**
광주대학교 물류유통경영학과*, 충북대학교 경영정보학과**

A Study on the Security Requirement for Transforming Cloud Data Center : Focusing on N - Data Center

Jong-Hei Ra*, Jae-Sook Lee**
Dept. of Logistics & Distribution, Gwangju University*
Dept. of Management Information System, Chungbuk University*

요 약 N데이터센터는 정부부처를 대상으로 클라우드 컴퓨팅 서비스를 제공하는 '클라우드 컴퓨팅센터'로 변모를 꾀하고 있으며, 각 부처에 필요한 만큼 정보자원을 서비스 형태로 제공하는 'IT서비스 센터'로 탈바꿈 예정이다. N센터 8중의 보안체계 하에서 클라우드서비스가 이미 정부부처에 제공되고 있으며, 향후 보안을 전제조건으로 민간분야까지 확대할 계획이다. 따라서 보안은 민간분야와의 클라우드 확산에 있어 선결요건이며, 이의 체계적이고 효율적 추진을 위해서 클라우드 데이터 센터로서의 보안수준을 파악하고 적절한 방안을 제시할 필요가 있다. 본 연구에서는 이를 위해 선진 각국의 클라우드 데이터 센터의 보안 요건을 분석하고 클라우드 서비스 형태에 클라우드 컴퓨팅의 취약점을 파악하고, 선진 민간 클라우드 데이터 센터의 보안수준을 파악하고, 현행 N데이터센터 보안 수준과 선진 민간 클라우드 데이터센터와의 갭을 분석하여 보안관점에서 전환을 위한 요건을 제시하였다.

주제어 : 클라우드, 데이터센터, 클라우드 데이터센터, 보안요건, 보안수준

Abstract N-Data Center which provide of cloud computing service for the Government departments, will be prepared transforming to cloud data center and transformed into an 'IT service' provided as a service to the information resources required by each department. N-Data center already provide a cloud service to the departments as maintains a high level of security, and plan to connecting with the private sector as a precondition of security. Therefore, in order to promote them effectively, it is necessary to determine the level of security in the cloud data center, and we have proposed appropriate measures. In this paper, we analyze security requirements of cloud data centers in developed countries and identify the leading private cloud data center security. In addition, we identify the N-data center security level, and analyzes the data center and private cloud gap and provide a transition strategy in terms of security finally.

Key Words : Cloud, Data center, Cloud Data Center, Security Requirement, Security Levels

* 본 논문은 2014년 광주대학교의 학술연구비에 의하여 지원되었음
Received 7 September 2014, Revised 15 October 2014
Accepted 20 November 2014
Corresponding Author: Jong Hei Ra(Gwangju University)
Email: jhra@gwangju.ac.kr, jslee480@naver.com

ISSN: 1738-1916

1. 서론

정보기술이 보편화되면서 전략적 도구로써의 중요성이 감소되고 있지만, 조직 운영을 위한 기반구조(Infrastructure)로 인식되고 있다. 그러나 정보기술 이용에 소요되는 비용 증가와 정보기술의 복잡성으로 인한 관리의 어려움으로 기업은 정보기술을 내부에 구축 및 보유하던 방식에서 전문기업이 제공하는 정보기술을 이용하는 형태로 변화하고 있다. 이러한 패러다임의 변화에 가장 적합한 모델이 클라우드 컴퓨팅 서비스이다. 2000년대 후반에 클라우드 서비스가 등장한 이후 아마존, 구글, IBM, 마이크로소프트 등 주요 IT 기업들이 클라우드 컴퓨팅 서비스를 제공하고 있으며, 페이스북, 유튜브, 마이스페이스 등은 인터넷 사용자를 위한 클라우드 서비스를 제공하고 있다. 클라우드 컴퓨팅 서비스는 사용자의 위치나 장치에 무관하게 사용자요구를 바탕으로 준비된 모든 프로세스들과 응용으로 클라우드 자원을 서비스하며, 빠르게 분배되고 용이하게 조정이 가능하다는 장점을 갖는다. 이로 인해 IT 조직들은 서비스 전송 효율성과 IT관리 역량 향상을 꾀할 수 있으며, 수시로 변화하는 고객의 비즈니스 요구에 신속하고 빠른 서비스를 제공할 수 있게 된다[1].

정보서비스 임대 현상을 대표하는 클라우드 컴퓨팅의 확산은 사용자뿐만 아니라 IT산업 전반에 큰 영향을 미치고 있다. 즉, 정보서비스 방식의 전환은 서버, 네트워크, 하드디스크 등을 구매하고 정보시스템을 직접 구축하는 전통적인 방식이 간편하고 저렴한 임대 계약으로 대체될 수 있기 때문이다. 클라우드 서비스로 전환은 비용의 절감뿐만 아니라 전문기업이 미리 구축한 서비스 또는 서비스 컴포넌트를 이용하여 기업에 필요한 정보서비스를 신속하게 만들 수 있어 기업의 민첩성을 증가시킬 수 있는 장점을 가지고 있다[2].

이와 같은 클라우드 컴퓨팅은 인터넷을 통하여 제공되는 어플리케이션들과 이 서비스들을 제공하는 기반이 되는 데이터센터 내의 모든 하드웨어와 소프트웨어를 포함하는 것으로 클라우드 컴퓨팅에 기초한 서비스는 몇 가지 특징을 지니고 있다. 먼저 인터넷이라는 공개된 환경에서 적용되고 표준화된 기술을 사용하여 유연성과 확장성이 높다. 또한 기존의 정보서비스와 구별되는 가장 큰 특징으로는 사용자의 요구에 의해 서비스를 변형할 수 있는 온-디멘드(On- demand)적인 성격이다.

클라우드 컴퓨팅은 서비스 제공 및 사용방식의 다양성으로 인하여 아직까지 범위나 개념이 명확하지 않다. 따라서 클라우드를 정의하기는 어렵지만 클라우드 서비스 특성을 기준으로 NIST나 가트너와 같은 연구기관의 정의가 많이 활용되는데 가트너는‘인터넷 기술을 활용하여 다수의 고객들에게 높은 수준의 확장성을 가진 자원들을 서비스로 제공하는 컴퓨팅의 한 형태’로 정의하고 있으며, NIST는 ‘구성 가능한 컴퓨팅 자원의 공유 풀을 필요할 때 편리하게 네트워크를 통해 접속할 수 있도록 하는 모델로 컴퓨팅 자원은 최소의 관리 노력이나 서비스 사업자와의 상호 작용으로 신속하게 공급되고 제공 가능’으로 정의하고 있다.

클라우드 컴퓨팅을 이용하기 이전의 기업들은 IT 인프라스트럭처에 대한 외부로부터의 침입 방지와 내부 모니터링을 통해 안정적으로 운영되는 데에 주력해 왔다. 하지만 클라우드 컴퓨팅으로 IT 인프라스트럭처의 범위가 기업의 외부까지 확대되면서 보안과 안정성이 핵심 요소로 부상하고 있다. 비록 클라우드 컴퓨팅은 전문기관에 의해 제공됨에 따라 데이터를 보호하기 위해 전문 인력과 자원을 이용한 관리로 개별 기업이나 개인이 직접 데이터를 관리하는 것보다 안전성이 높은 것이 일반적이다. 하지만 사용자의 입장에서는 민감한 데이터에 대한 직접적인 통제 권한을 포기해야 하며, 클라우드 컴퓨팅 사고 시 기업에 미치는 피해의 파급효과가 크기 때문에 정보자원의 가용성과 보안 측면에서 도입의 거부감이 존재한다. 즉, 클라우드 컴퓨팅은 소프트웨어 및 데이터와 정보까지 외부에서 서비스로서 제공되기 때문에 정보 유출의 가능성이 열려 있으며, 제공자의 정전이나 과부하로 다운되는 피해 발생의 우려가 존재한다.

또한, 기술적인 측면에서도 클라우드 컴퓨팅 서비스는 웹을 기반으로 하면서 정보자산의 관리주체 및 장소, 그리고 네트워크를 통한 공유 등으로 관리해야할 보안 대상과 기술이 다양하고 복잡화되고 있다. 특히, 웹 어플리케이션의 취약성을 이용한 해킹이 전체의 75%를 차지할 정도로 기존의 보안 위협과 상이한 경향을 보이고 있다. 이와 같이 클라우드 서비스에서는 서비스 제공자의 신뢰, 웹 위협, 법적 기준/제약, 데이터 누출, 분산된 인프라스트럭처, 공유된 인프라스트럭처 등의 위험요인이 증가하고 있다. 이를 반증 하듯, IDC 조사에 따르면, 244명의 IT

관련 임원들을 대상으로 IT 클라우드 서비스 활용의도에 대한 설문조사 한 결과, 보안이 가장 중요한 과제로 선정되었다[3].

한편, N-데이터센터는 정부부처를 대상으로 클라우드 컴퓨팅 서비스를 제공하는 '클라우드 컴퓨팅센터'로 변모를 꾀하고 있으며, 각 부처에 필요한 만큼 정보자원을 서비스 형태로 제공하는 'IT서비스 센터'로 탈바꿈 예정이다. 따라서 본 연구에서는 이를 위해 선진 각국의 클라우드 데이터 센터의 보안 요건을 분석하고 클라우드 서비스 형태에 클라우드 컴퓨팅의 취약점을 파악하고, 선진 민간 클라우드 데이터 센터의 보안수준을 파악하고, 현행 N데이터센터 보안 수준과 선진 민간 클라우드 데이터센터와의 갭을 분석하여 보안관점에서 전환을 위한 요건을 제시하고자 한다.

2. 이론적 배경

2.1 클라우드 서비스

클라우드 컴퓨팅은 매년 20%씩 성장하고 있으며 2013년 전체적인 시장 규모는 590억 달러에 달하고 있다. 이러한 클라우드 컴퓨팅을 구현하는 방식은 매우 다양하다. 가장 일반적인 방식은 <Table 1>에서와 같이 IaaS, PaaS, SaaS 등 세 가지이다.

〈Table 1〉 Cloud Service Type

Type	Concept
IaaS	The service that be provide user for the computing resource such as processing, storage, network in order to deploy operating systems and application software.
PaaS	The service that deploying to user on the cloud infrastructure that use the application that is new creating or have already created by the supported programming languages, libraries, services, tools.
SaaS	The service that provide the user for applications running in the cloud infrastructure.

비즈니스를 수행하는 조직에서는 클라우드 컴퓨팅서비스를 통해서 조직의 정보기술 실현하기 위한 비용구조를 자본비용 지출(CapEx : Capital Expenditure)로부터 운영비용 지출(OpEx : Operational Expenditure)로 전환하기 위한 적절한 방법을 찾는 것이다. 제공서비스는 퍼블릭 클라우드, 프라이빗 클라우드, 하이브리드 클라우드 등 서비스 모델로 구분할 수 있다[4].

2.2 데이터센터(Data Center)

오늘날 대부분의 기업이나 조직에 있어서 데이터 센터는 비즈니스(business)의 핵심으로 여겨지고 있다. 데이터센터는 비즈니스의 운영과 고객을 위한 핵심적인(Mission Critical) 애플리케이션 및 서비스를 지원한다. 이러한 데이터센터는 발전정도에 따라 물리적인 데이터센터, 가상화된 데이터센터, 인프라스트럭처 클라우드, 하이브리드 클라우드로 4단계로 구분할 수 있다. 1단계는 물리적인 데이터센터로 전통적인 데이터센터를 지칭한다. 서버시스템, 스토리지 시스템 그리고 네트워크 시스템, 관련 소프트웨어 시스템 등을 포함하는 모든 시스템들이 동일한 물리적인 공간 내에 존재한다. 시스템은 물리적인 장치에 따라 독립적으로 운영되며, 낮은 자원의 활용도, 개발 및 관리의 어려움 등의 단점을 갖는다. 2단계는 가상화된 데이터센터이다. 데이터센터는 가상화 기술을 이용하여 물리적인 장치를 '분리'한다. 따라서 물리적으로 단일 장치는 상위 수준의 응용프로그램에 투명하게 서비스를 제공하기 위하여 여러 개의 독립적인 장치로 가상화될 수 있다. 이러한 가상화는 대상에 따라 서버 가상화, 스토리지 가상화, 네트워크 가상화, 플랫폼 가상화 등으로 구분할 수 있다. 가상화 기술은 자원의 활용도의 현저한 개선, 시스템 투자비용의 절감, 데이터센터 운영에 소모되는 에너지의 절감, 운영의 유연성 향상 및 운영비용을 절감 등 데이터센터의 총소유비용(TCO)을 줄이는데 기여한다. 3단계는 인프라스트럭처를 클라우드로 서비스하는 데이터센터이다. 클라우드 기술이 성숙함에 따라 데이터센터는 클라우드 다양한 사설 인프라스트럭처 클라우드를 구축하기 위하여 클라우드 컴퓨팅 기술을 활용하기 시작하였다. 마지막 4단계는 프라이빗 클라우드와 블릭 클라우드를 동시에 제공하는 하이브리드 클라우드 데이터센터이다.

2.3 클라우드 데이터센터의 보안 위협

클라우드의 신뢰할 수 있는 접근은 클라우드 컴퓨팅의 장점을 보장할 수 있으며, 따라서 클라우드 데이터센

터의 구축 시 신뢰에 대한 고려가 필수적이다. 클라우드 센터의 정보 네트워크 및 시스템에서는 보안 제어를 통해 정보의 기밀성(Confident), 무결성(Integrity) 및 가용성(Availability) 문제를 처리한다. 조직들이 점차 애플리케이션, 데이터 및 기타 자원을 소수의 대형 데이터센터로 통합함에 따라 단일 시스템 보안 침해로 인한 위험도 높아지고 있다[5]. 단일 서버는 전통적으로 하나의 애플리케이션을 수용하는 반면, 오늘날의 가상화된 서버는 여러 애플리케이션이나 컴포넌트를 수용한다. 따라서 한 대의 물리적 서버에서 성능의 저하가 발생하는 경우에 많은 애플리케이션과 사용자들에게 크나큰 영향을 미치게 된다. 특히 현대의 데이터 센터는 클라우드 서비스 제공을 위해 새로운 기술 요소들이 부각되면서 전에 없던 중대한 보안 문제가 발생한다. 이러한 보안 문제를 유발하는 대표적인 형태가 서버 가상화, 분산된 애플리케이션 아키텍처, IP 기반 스토리지 네트워크, 봇넷(Bootnet)을 이용한 DoS 공격 등 네 가지이다[6][7][8].

첫 번째, 서버가상화의 문제이다. 서버 가상화는 기업이 서버 자원을 최대한 활용하고 설치 공간, 전기 및 냉각 요구 수준을 낮출 수 있도록 지원하는 등 데이터센터 통합에 중요한 역할을 해 왔으나 가상기계(Virtual Machine) 내부와 가상기계 간에 수행되는 모니터링 및 제어가 어려워지면서 새로운 유형의 중대한 보안 위험을 수반한다.

둘째, 분산된 애플리케이션 아키텍처 문제이다. 클라우드 환경에서는 기존의 모놀리식(monolithic) 애플리케이션 개발에서 탈피해 재사용 가능한 공통의 서브 컴포넌트를 기반으로 하는 분산 애플리케이션 아키텍처로 전환하는 중대한 변화가 이루어진다. 분산 애플리케이션 아키텍처는 보다 신속하면서도 효율적인 애플리케이션 개발을 가능하게 하지만, 트랜잭션 당 여러 플로우를 수용하는 고도로 분산된 통신 패턴을 생성함으로써 새로운 보안 위험을 야기할 수 있다.

셋째, IP 기반 스토리지 네트워크에 따른 문제이다. 유연성 및 비용 이점으로 많은 기업들이 IP 기반 스토리지 기술을 구축하고 있으나 IP 네트워크 기반의 스토리지를 구축하면 보안 위험이 높아질 수 있다.

넷째, 봇넷을 이용한 DoS 공격이다. 사이버 공격이 점차 빈번하게 발생하고 더욱 교묘해지고 있는 상황에서 심각하면서도 지속적인 보안 문제가 나타나고 있다. 과거에는 악의적 해커가 "해커" 사회에서 자신의 존재를 과시하기 위해 시스템을 무작위로 공격하였으나 오늘날에는 브라우저 기반의 "클라우드" 컴퓨팅, 모바일 데이터 플랫폼 및 소셜 네트워킹이 하나로 결합되면서 신종 위협이 증가한다.

3. 연구방법론

본 연구의 연구방법으로 FGI(Focus Group Interview)를 채택하였다. FGI는 공통적인 특징을 가진 전문가들이 특정 주제에 대하여 집중 토론을 하여 조사를 진행하는 방법으로 설문구성을 위한 예비조사, 복잡한 행동이나 동기 부여와 관련된 내면적인 요인을 발견하기 위한 탐색적인 연구, 그리고 연구문제에 대한 해답을 도출하는 독자적인 연구 등의 목적으로 사용될 수 있다. 즉, FGI는 소규모 참여자간에 경험이나 의견을 표현하고, 집단토론 과정에서 즉흥적인 질문이나 반응을 허용함으로써 다양하고 심도 있는 의견의 수렴이 가능한 연구기법이다.

이와 같은 특성으로 인하여 FGI는 잘 알려지지 않은 주제나 현상을 이해하는 방법으로 사용되며, FGI의 결과로 정리된 참여자간의 상호작용이나 토론을 통해 나타난 집단전체의 의견은 개인 의견의 총합이상이고, FGI과정에서 의견 형성에 대한 관찰을 통해 결정요인에 대한 정보를 충분하게 수집할 수 있다. 체계화된 구조가 존재하는 새로운 분야에서는 양적 분석을 통한세부적인 내용을 파악하기에는 한계가 있으므로, 계량적인 분석보다는 심도있는 인터뷰, 문헌분석을 통한 직접관찰과 같은 정성적인 분석방법이 보다 적합하며, 전문가가 많지 않은 본 연구주제와 같은 경우 소규모 집단을 대상으로 한 FGI 방법이 타당한 것으로 보인다. 이에 본 연구는 FGI를 통한 공공 클라우드 서비스모델을 도출하기 위해 준비단계, FGI 계획, 그리고 FGI 실시단계로 구분하여 수행하였다. 준비단계에서는 본 연구의 주제영역인 클라우드 데이터센터의 보안과 관련된 자료를 인터넷 및 문헌조사를 이용하여 수집하였다.

조사된 자료에 대한 분석 작업을 통해서 클라우드 데이터센터의 보안에 대한 개념과 기존 사례들을 정리하였다. FGI 계획단계에서 FGI에 참여자, 분석자, 사회자등 FGI 진행자와 참여자 집단의 크기나 충분성, 참여자의

발표유도방안, 정리주체 및 방법 등 FGI 역할별 고려요소를 반영하여 계획을 수립하였다. 특히 중요한 참여자 구성은 연구주제의 특수성을 감안하여 클라우드 관련분야에 풍부한 경험을 보유한 5명의 전문가들로 구성하였다. FGI는 2014년 3월부터 약 3개월간 7번 실시하였다. FGI주제에 따라 합의에 이를 때까지 반복적인 FGI를 수행하였으며 사회자가 이를 종합하여 클라우드 데이터센터로의 전환을 위한 보안요건을 확정하는 과정을 거쳤다.

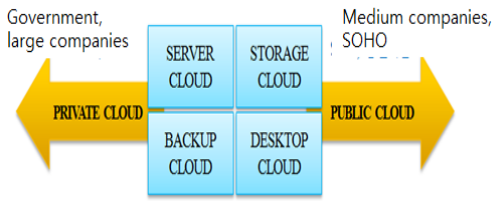
4. 클라우드 데이터센터로의 전환을 위한 보안요건

4.1 국내외 주요 클라우드 데이터센터의 보안

N데이터센터가 클라우드 데이터센터로 전환하기 위해 고려해야 하는 보안성을 분석하기 위해서는 대표적인 클라우드 서비스 사업자에 대한 보안성을 분석할 필요가 있다. 이를 위해 국내 주요 클라우드 서비스 사업자인 L-클라우드 서비스와, 국외 주요 클라우드 서비스 사업자인 Amazon과 Google의 보안성 분석 결과를 제시한다. 이와 함께 현재까지 발생한 주요 클라우드 보안 사고 사례를 통해 중점적으로 대비해야 할 보안성을 분석한다.

4.1.1 L 클라우드 데이터센터

L사는 2002년 유틸리티 컴퓨팅을 시작한 이후, 2008년부터 그룹 계열사의 IT 자산을 인수, 운영함으로써 클라우드 서비스를 제공하기 시작하였으며, 2011년 퍼블릭 클라우드 서비스를 시작하였다. 초기에는 IaaS 중심의 서비스에서 현재는 PaaS, SaaS로 서비스 영역을 확대하고 있다. [Fig. 1]에서와 같이 L사의 프라이빗 클라우드 서비스는 일반 PC 환경을 VDI환경으로 전환하며, 퍼블릭 클라우드 서비스는 vDataCenter, vStorage를 포함하는 IaaS, vDesktop과 같은 PaaS, 그리고 그룹웨어, ERP, CRM 등을 제공하는 SaaS로 구성된다[9].



[Fig. 1] Cloud Service of L Company's Case

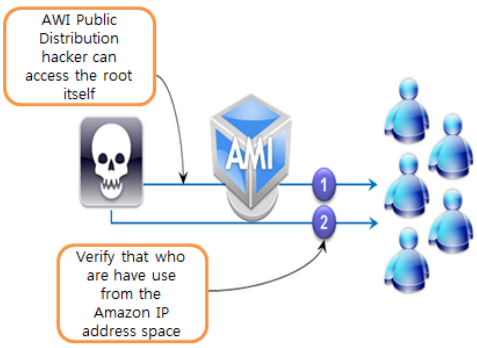
4.1.2 아마존 클라우드 데이터센터

EC2는 사용자에게 가상 서버를 제공하는 아마존의 대표적인 IaaS이다. Amazon은 EC2, S3, EBS(Elastic Block Store), SQS(Simple Queue Service) 등 다양한 클라우드 서비스를 제공하고 있으며, 전 세계에 데이터센터를 운영하고 있다. 이러한 아마존 서비스는 보안측면에서 AMI(Amazon Machine Image), 악성코드 방지(Malware Prevention), 원치 않는 연결(Unsolicited Connections), 기계 지문인식(Machine Fingerprinting) 등 네 가지 주요한 기능을 제공하고 있다[10].

첫째, AMI(Amazon Machine Image)이다. 사용자는 서버에 AMI를 실행할 수 있으며, 아마존은 다양한 종류의 AMI(웹서버, 웹애플리케이션, 데이터베이스 등)를 선택할 수 있도록 제공한다. 또한, AMI는 실제 동작중인 시스템, 가상머신 이미지, 또는 다른 AMI를 Amazon S3에 복사하여 생성할 수 있으며 이를 번들링(bundling)이라고 부른다. AMI는 Amazon에서 제공할 수도 있고, 개인이 공개할 것일 수도 있으며, 기업에서 사용하는 것일 수도 있다. AMI가 시작되면 Amazon API를 통해 DNS 주소가 공개되고 포트 22번의 SSH(Linux인 경우) 또는 포트 3389번의 원격데스크톱(Windows인 경우)을 이용하여 접근할 수 있다.

둘째, 악성코드 방지(Malware Prevention)이다. AMI의 파일시스템을 오픈소스 안티바이러스 엔진인 ClamAV로 점검한 결과 2개의 AMI에서 Trojan-Spy와 Trojan.Firepass 악성프로그램이 발견되었다. 이는 가상머신 이미지의 일종인 AMI가 악용될 수 있음을 보여주는 사례이지만 클라우드 서비스 제공자가 탐지하기는 매우 어렵다.

셋째, 원치 않는 연결(Unsolicited Connections)이다. 실행된 AMI로부터 외부로의 불필요한 접속 요청은, 백도어, 악성코드 감염 등일 수 있기 때문에 보안상 점검해야 할 사안이지만, 정상 소프트웨어의 업데이트 확인 등과 구별하는 것은 거의 불가능하다.



[Fig. 2] Image Certification using Fingerprinting

넷째, 기계 지문인식(Machine Fingerprinting)이다. [Fig.2]에서와 같이 취약한 AMI를 이용할 경우 공격자는 해당 AMI에 무단 접속할 수 있지만, 먼저 대상 시스템을 파악해야 하며, 이러한 파악 과정을 지문인식(Fingerprinting)이라고 한다. 예를 들어 해커는 자신이 root 접속할 수 있는 SSH 키를 은닉한 AMI를 공개적으로 배포한 후 이를 사용하는 사용자의 가상머신에 은밀하게 접속할 수 있다. 이 때 해커는 전체 아마존 IP 주소 대역에서 누가 자신의 이미지를 사용하고 있는지 확인해야 한다. 이미지를 확인하는 방법은 크게 SSH 키 일치 확인, 서비스 일치 확인, 그리고 웹 일치 확인 등이 있다. 만약, 아마존과 마찬가지로 가상머신 이미지를 일반 사용자가 공개할 수 있도록 한다면, 이에 대한 보안대책을 충분히 고려해야 할 것이다.

4.1.3 Google 클라우드 데이터센터

구글은 Google Apps를 통해 IaaS, PaaS, SaaS 등 모든 형태의 클라우드 서비스를 제공하고 있으며, 공식적으로는 전세계 13곳에서 데이터센터를 운영중에 있다. 이러한 구글의 클라우드 데이터 센터 역시 아마존의 클라우드 데이터 센터와 유사하게 보안성 강화를 위하여 관리적 측면에서 데이터 자산관리(Data Asset Management), 악성코드방지(Malware Prevention), 모니터링(Monitoring), 취약점 관리(Vulnerability Management) 등을 제공하고 있다[11][12].

첫째, 데이터 자산관리(Data Asset Management) 기능이다. 내부 데이터를 포함하여 사용자 데이터에 대한 관리는 보안 정책 및 정의된 절차에 따라 진행된다. 또한, 데이터는 지역적으로 분산된 데이터센터에 분산/백업 저장되며, 각 사용자마다 서로 다른 분산 저장 구조를 갖도록 설계하였다.

둘째, 악성코드방지(Malware Prevention) 기능이다. 악성코드는 개인 사용자 뿐만 아니라 클라우드 서비스 제공자에게도 매우 위협적인 요소이다. 특히, 가상화에 기반한 서비스 제공시 기존 악성코드 탐지 기법을 적용하기 어려운 측면이 있다. 구글은 웹사이트에 대한 자사의 검색 인덱스를 활용하여 자동화된 스캐너를 운영하고 있다. 웹사이트가 대다수의 악성코드 배포 수단이긴 하지만, 클라우드 서비스를 제공할 경우 다른 침입 경로에 대한 대비도 필요하다.

셋째, 모니터링(Monitoring) 기능이다. 구글은 네트워크의 트래픽 분석, 시스템에 대한 내부자의 행동, 그리고 외부의 알려진 취약점 정보 등을 분석하는 보안 모니터링 프로그램을 시행하고 있다. 네트워크 내 다양한 지점에서 내부 트래픽을 감시하여 봇넷 연결과 같은 의심스러운 행동을 탐지한다. 이를 위해 구글은 상용 소프트웨어는 물론이고 공개 소프트웨어도 함께 이용하며, 구글이 자체 개발한 “상관관계 시스템(Correlation System)”도 활용한다.

넷째, 취약점 관리(Vulnerability Management) 기능이다. 취약점에 즉각 대응하기 위해 별도의 보안팀(Google Security Team)을 운영한다. 보안팀은 상용 소프트웨어 이외에 자체 개발한 소프트웨어를 이용하여 자동/수동 침입 시도, 품질 보증, 소프트웨어 보안 검토 및 감사를 진행한다. 또한 구글은 자체 서비스에 대해 취약점을 신고하는 사용자에게 적절히 보상하는 “취약점 보상 프로그램(Vulnerability Reward Program)”을 2010년부터 운영중이다.

4.2 클라우드 서비스 보안 사고 사례(2013)

아마존을 비롯하여 구글 등 대표적인 클라우드 서비스 제공자의 보안 사고는 <Table 2>에서와 같이 2013년 한 해 동안 수차례 발생하였다. 이들 보안사고의 대부분은 정전 등 외부적인 요인에 의했거나 내부 직원의 실수 등에 의해 발생하였다. 따라서, 주요 클라우드 서비스 제공자의 보안 사고 사례를 분석했을 때, 클라우드 데이터센터 운영 시 가용성 증대 방안 마련에 초점을 맞춰야 할 것으로 보인다.

〈Table 2〉 Cloud Services Accident Case(2013)

Time	Cause	Service Provider	Symptom
2013.01	Internal Management	Amazon	Can not connect the site
2013.01	Unknown	Dropbox	Can not upload files and syn files
2013.01	DNS error	Facebook	Can not connect the site
2013.02	Internal Management	Microsoft	Can not connect the Office365, Outlook, Bing
2013.02	SSL Certificate	Microsoft	Windows cloud Storage error
2013.03	Internal Management	Google	Can not connect the Google Drive
2013.05	Unknown	Dropbox	Can not upload files and syn files

4.3 클라우드 데이터센터로의 전환 시 고려요소

4.3.1 가상화에 따른 보안 대책

클라우드 데이터센터는 물리적 자원 가상화, 하이퍼바이저, VM 운영/관리, 가상화 자원 모니터링, 가상화 네트워크 통신 등과 같은 새로운 가상화나 분산화 기술을 활용하는 등 기존 데이터센터 운영과는 다른 측면이 있다. 때문에 이들 신기술 적용에 따른 보안성을 파악하고 적절한 보안수준의 유지를 고려해야 한다. 따라서 기존 물리적인 시스템 기반의 보안 솔루션만으로는 불충분할 수 있기 때문에 가상화 및 분산화를 고려한 적절한 보안 솔루션을 도입해야 한다.

4.3.2 가용성과 무결성

클라우드 서비스에 대한 주요 장애 유형을 분석해보면 해킹에 따른 정보 유출이나 서비스 장애보다는 내부 관리 부주의 또는 H/W, S/W 오류, 천재지변 등에 의한 가용성 문제가 대부분을 차지하고 있다. 특히, 서비스 장애로 인한 데이터 손실도 가용성을 저하시키는 요인이 될 수 있으며, 고객사의 주요 정보가 노출(프라이버시)되거나 훼손(무결성)을 유발할 수도 있다. 이에 대한 대비책으로는 서비스 운영 매뉴얼 구축 및 준수, 장애 발생 시 조치 사항 등을 사전에 완벽하게 준비할 필요가 있으며, 가용성을 100% 유지하는 것은 현실적으로 불가능하기 때문에 구글의 Apps Status Dashboard처럼 장애 및 복구와 관련된 정보를 투명하게 공개하는 것도 고려할 필요가 있다. 단, 사용자 정보의 무결성 유지는 반드시 필요하기 때문에 다중 백업에 대한 고려가 있어야 한다.

4.3.3 퍼블릭 클라우드 제공에 따른 경계 구축

N데이터센터의 경우 정부기관을 상대로 프라이빗 클라우드 서비스를 제공하고 있으며, 이를 일반 사용자를 대상으로 한 퍼블릭 클라우드 서비스로 확대할 예정이다. 특히 프라이빗 클라우드 서비스 제공시 확장성을 고려하여 외부의 퍼블릭 클라우드를 이용한 하이브리드 클라우드 서비스 구축을 고려할 수 있다. 외부 퍼블릭 클라우드 이용 시 보안을 고려하여 중요도는 낮고 대용량인 데이터를 우선적으로 고려해야 해야 한다. 정부기관을 대상으로 한 프라이빗 클라우드 서비스 이외에 일반 사용자를 대상으로 한 퍼블릭 클라우드 서비스 제공시 프라이빗 클라우드와의 경계 구축을 강화해야 한다. 특히, 민간 클라우드 서비스 제공자와는 달리 정부에서 제공할 경우 이에 대한 대비책을 확실히 할 필요가 있다.

4.3.4 자체 보안 전문 인력 보유

N데이터센터가 퍼블릭 클라우드 서비스를 제공할 경우 다른 주요 사업자와 비교했을 때 자체 보안 전문 인력이 부족하다. 보안 전문 인력의 대부분이 협력 업체 직원이며, 계약 관계에 따라 인력 변동이 심한 편이므로 보안 사고 발생에 대한 대비 및 계획 수립에 어려움이 있다.

4.3.5 클라우드 서비스 악용 방지(CaaS 방지)

해킹 기술의 경우 난이도는 점차 낮아지는 반면 피해 규모는 점차 커지고 있다. 특히 클라우드 서비스의 확대로 인해 해킹에 필요한 자원을 언제든 필요에 따라 임대할 수 있게 되면서 해킹 비용 역시 낮아지고 있다. 예를 들어, 9자리 패스워드 크랙에 아마존 EC2와 같은 클라우드 컴퓨팅을 이용할 경우 소요 비용이 $87에 불과할 것으로 나타나고 있다. 또한, 여러 대의 가상 서버를 임대하여 DoS 공격을 시도할 경우 수 십 달러 내외로 소규모 회사에 피해를 입힐 수 있을 것으로 예측된다. 실제로 지난 2011년 5월, 소니 해킹 사고 발생 시 아마존의 EC2가

〈Table 3〉 Compare of Cloud Data center

Service Provider	Service	Virtualization	Availability/ Integrity	perimeter security	manpower	Preventing CaaS
L Cloud	SaaS PaaS IaaS	YES	YES	YES	HIGH	NO
Google Cloud	SaaS PaaS IaaS	YES	YES	YES	HIGH	NO
Amazon Cloud	SaaS PaaS IaaS	YES	YES	YES	HIGH	NO
N-Data center	**IaaS PaaS**	**YES**	**YES**	**YES**	**LOW**	**NO**

이용된 것으로 알려져 있다. 따라서 기존 해킹을 방어하기 위한 대응책 이외에 해킹의 진원지가 될 수도 있기 때문에 이를 탐지하기 위한 기술이 필요하다.

5. 결론

N데이터센터는 정부부처를 대상으로 클라우드 컴퓨팅 서비스를 제공하는 '클라우드 컴퓨팅 센터'로 변모를 꾀하고 있으며, 각 부처에 필요한 만큼 정보자원을 서비스 형태로 제공하는 'IT서비스 센터'로 탈바꿈 예정이다. 본 연구에서는 선진 각국의 클라우드 데이터 센터의 보안 요건을 분석하고 클라우드 서비스 형태에 클라우드 컴퓨팅의 취약점을 분석하고, 선진 민간 클라우드 데이터 센터의 보안수준을 파악하였다. N데이터센터 보안수준과 선진 민간 클라우드 데이터센터와의 갭을 분석하여 전환 시 고려요소로 가상화에 따른 보안 대책, 가용성과 무결성, 퍼블릭 클라우드 제공에 따른 경계 구축, 자체 보안 전문 인력 보유, 클라우드 서비스 악용 방지(CaaS 방지) 등 5가지 보안요건을 제시하였다.

첫째, 가상화 측면에서는 클라우드 서비스에서 가상화가 차지하는 비중은 매우 높으며, 이에 대한 보안 솔루션도 출시되어 있으나, N데이터센터의 구축 환경에 맞는 솔루션을 충분히 검토할 필요가 있다. 둘째, 가용성측면에서 다양한 보안성 가운데 주요 보안 장애 사례에서 보듯이 가용성 확보가 가장 큰 문제로 부각되고 있다. 따라서 가용성을 높일 수 있는 보안 대책을 마련해야 하며, 가용성 저하가 무결성에 영향을 미치지 않도록 백업 등의 대책을 수립해야 한다. 셋째, 퍼블릭 클라우드 제공에 따른 경계 구축측면에서는 N데이터센터는 정부 기관을 대상으로 한 프라이빗 클라우드 서비스를 이미 제공하고 있으며, 퍼블릭 클라우드 서비스를 제공할 계획으로 있기 때문에 이에 대한 명확한 경계 구축(네트워크 분리 등)이 필수적이다. 넷째, 국내•외 민간 클라우드 서비스 사업자의 경우 자체 보안 인력을 갖추고 있는 것으로 보이며, 자체 보안 솔루션을 운영하는 경우도 있다. N데이터센터는 현재 외부 협력사에 대한 의존도가 높은 편이므로 자체 보안 인력을 확보할 필요가 있다. 마지막으로 CaaS 방지는 현재 특정 솔루션이 존재하지 않는다. 다만, 클라우드 서비스가 악용됨을 탐지하는 탐지솔루션은 적용할 수 있을 것으로 보이며, 사용자 인증, 인가, VDI 활용 모니터링 등을 통해 탐지 및 대응력을 높일 필요가 있다.

ACKNOWLEDGMENTS

This research was supported by the Academic Research Fund of Gwangju University in 2014.

REFERENCES

[1] Armbrust, Michael, Armando Fox, Rean Griffith, Above the Clouds: A Berkeley View of Cloud Computing, Berkeley EECS Department, University of California, 2008.

[2] Buyya, Rajkumar, Chee Shin Yeo,Srikumar Venugopal, Market-oriented cloud computing: Vision, hype, and reality for delivering it services as computing utilities, International Conference on High Performance Computing and Communications, 2008.

[3] IDC, IT Cloud Services User Survey, pt.2: Top Benefits & Challenges ,2008.

[4] NIST Special Publication 800-145, The NIST Definition of Cloud Computing, 2011.

[5] DANISH JAMIL, HASSAN ZAKI, CLOUD COMPUTING SECURITY," International Journal of Engineering Science and Technology, 3(4), pp3478~3483, 2011.

[6] Vaquero L, Rodero-Merino L, Mor D, Locking the sky: a survey on IaaS cloud security, Computing, 91, pp93 - 118, 2011.

[7] R. Chow, P. Golle, M. Jakobsson, E. Shi, et. al, Controlling data in the cloud: outsourcing computation without outsourcing control. Proceedings of the 2009 ACM Workshop on Cloud Computing Security, 2009.

[8] Pearson, S., Taking account of privacy when designing cloud computing services, In ICSE Workshop on Software Engineering Challenges of Cloud Computing, Vancouver, Canada, pp44-52, 2009.

[9] LG CNS, "Introduction of LG CNS Public Cloud", http://cloud.lgcns.com/

[10] M.Balduzzi, J.Zaddach, D.Balzarotti, E.Kirda, and S.Loureiro, A Security Analysis of Amazon's Elastic Cloud Service.Proceeding SAC '12 Proceedings of the 27th Annual ACM Symposium on Applied Computing, pp1427-1434, 2012.

[11] Google, "Google's Approach to IT Security, https://cloud.google.com/files/Google-CommonSecurity-WhitePaper-v1.4.pdf"

[12] https://cloud.google.com/files/Google-Common Security-WhitePaper-v1.4.pdf

나 종 희(Ra, Jong-Hei)

- 1990년 2월 : 성균관대학교 정보공학과(공학사)
- 1992년 2월 : 성균관대학교 정보공학과(공학석사)
- 2001년 8월 : 성균관대학교 정보공학과(공학박사)
- 2001년 9월 ~ 현재 : 광주대학교 물류유통경영학과 교수
- 관심분야 : 시스템성능, 클라우드 컴퓨터, 빅데이터 처리
- E-Mail : jhra@gwangju.ac.kr

이 재 숙(Lee, Jae-Sook)

- 1988년 2월 : 서울여자대학교 교육심리학과(교육학사)
- 2006년 2월 : 충북대학교 경영대학원(경영학석사)
- 2007년 3월 ~ 현재 : 충북대학교 경영정보학과 박사과정
- 관심분야 : SNS, 경영커뮤니케이션 IT벤처기업
- E-Mail : jslee480@naver.com