정 보 보 호 학 회 지
제26권 제1호, 2016. 2

기업의 하이브리드 클라우드 기술 활용 및 보안 동향

박 준 현*, 박 재 승**, 조 성 환***, 전 환 웅****, 전 은 정*****, 김 학 범******

요 약

하이브리드 클라우드는 클라우드 컴퓨팅의 구축모델 중 하나로, 일부 IT 리소스는 내부 프라이빗 클라우드를 통해 서비스로 제공하고 일부는 타사 서비스 공급업체가 퍼블릭 클라우드에서 제공하는 방식을 의미한다. 본 논문에서는 기업이 이러한 하이브리드 클라우드 기술을 어떠한 방식으로 제공하고 활용하는지에 대해서 기술할 것이며, 클라우드 보안 관련 동향에 대해서도 기술한다.

Ⅰ. 서 론

중간 규모의 기업과 대기업 및 정부기관은 비즈니스 대응 능력과 효율성을 최대한 높이고 경쟁력을 확보하기 위해 하이브리드 클라우드 환경을 구축하고 있다.

기존의 IT환경에서는 애플리케이션 소프트웨어와 지원 하드웨어를 개별적으로 구매, 관리 및 투자하고 보통 수개월에 걸쳐 구축한다. 반면 클라우드 컴퓨팅 환경에서는 다양한 IT 리소스를 몇 분 또는 몇 시간 내에 이용할 수 있으며 실제 사용량에 따라 비용이 청구된다.

클라우드는 클라우드 인프라의 운영 방식에 따라 퍼블릭 클라우드, 프라이빗 클라우드로 나뉜다([표 1] 참조).

하이브리드 클라우드는 내부 IT 부서의 최대 장점과 외부 IT 공급업체의 역량을 결합한 가장 유연하고 경제적인 클라우드 컴퓨팅 모델이다. 조직의 입장에서는 프로젝트를 보다 신속하게 착수하고 새로운 기능과 매출 기회를 빠르게 활용할 수 있으며 시장의 변화에 민첩하게 대응할 수 있으므로 클라우드 인프라스트럭처로 전환하면 IT 조직이 많은 비용을 수반하는 조직에서 전략적인 파트너로 탈바꿈하게 된다.

〔표 1〕 클라우드 컴퓨팅 유형별 특징

〔출처 : 정보통신정책연구원〕

구분	주요 특징
Public Cloud (공용 클라우드)	• 누구든지 이용 가능하도록 구현되는 것으로 일반 이용자 또는 대기업에게 사용량에 따라 과금하는 현태로 제공되는 서비스 • 퍼블릭 클라우드의 인프라는 서비스를 판매한 업체가 소유
Private Cloud (개인 클라우드)	• 특정 조직 내부에서 클라우드 컴퓨팅 사용 환경을 제공하여 폐쇄적으로 구현하는 서비스 • 프라이빗 클라우드 인프라는 해당기관 또는 제3자에 의해 관리할 수 있으며, 영역 내/영역 외에 사용자가 조직에 포함되는 여부에 따라 권한 할당이 가능함
Hybrid Cloud (혼합 클라우드)	• 퍼블릭 클라우드와 프라이빗 클라우드의 혼재된 형태로 중요자료는 프라이빗 클라우드에 보관하고, 부분적으로 퍼블릭 클라우드를 활용하는 형태로 운영 • 데이터와 애플리케이션의 이동을 가능하게 하는 표준기술로 하나로 묶거나 2개 이상의 클라우드를 통합함

하이브리드 클라우드는 퍼블릭 클라우드와 프라이빗 클라우드를 결합한 형태로서, 다음과 같은 일반적인 특성을 통해 IT 부서의 역할을 독점적인 서비스 제공자에서 IT 서비스의 "중개자"로 바꾸어 놓을 수 있다.

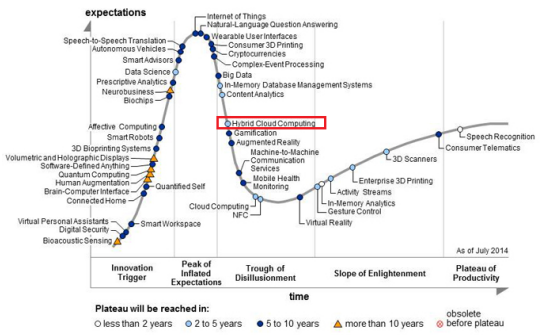
퍼블릭 클라우드 환경에서 IT 리소스는 타사 서비스 공급업체가 소유하고 관리하며 여러 고객이 공유하면서 인터넷을 통해 액세스한다. 높은 수준의 규모의 경제가 실현되기 때문에 비용이 저렴하지만 투명성과 제어 수준도 낮다[1]. 때문에 퍼블릭 클라우드는 미션 크리티컬

* 동국대학교 국제정보대학원 pcman00@hanmail.net
** 동국대학교 국제정보대학원 Supplay@nate.com
*** 동국대학교 국제정보대학원 sunghwan220@hanmail.net
**** 동국대학교 국제정보대학원 goldzx@naver.com
***** (주)이지제이 easyj@easyj.co.kr
****** 동국대학교 국제정보대학원 / 디지큐코리아㈜ khb0305@dongguk.edu

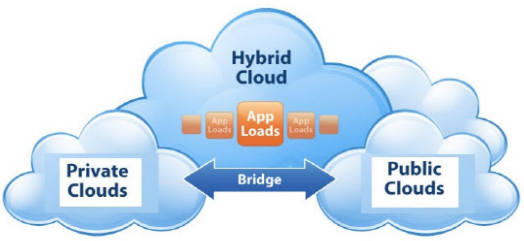
하지 않은 애플리케이션과 중요도가 낮은 정보에 종종 사용되고 있다. 가트너 그룹이 2014년 7월에 발표한 신기술 하이프사이클을 보더라도 하이브리드 클라우드는 이미 성숙해가고 있는 시점에 있다.

프라이빗 클라우드 환경에서는 단일 조직이 IT 리소스를 소유하고 내부적으로 공유하면서 전용으로 사용하며 리소스를 인터넷 또는 LAN을 통해 서비스로 제공하고 있다. 퍼블릭 클라우드 보다는 낮은 수준이지만 규모의 경제와 비용 절감 효과가 크고 투명성과 제어 수준이 높으며 멀티 테넌시와 관련된 문제도 해소된다. 따라서 미션 크리티컬한 애플리케이션과 중요 정보가 프라이빗 클라우드에 상주하는 경우가 많다.

일부 애플리케이션은 퍼블릭 클라우드 환경과 프라이빗 클라우드 환경 모두에 상주하기도 한다. 이 때 퍼블릭 클라우드는 필요에 따라 프라이빗 클라우드의 확장 솔루션 역할을 하며 급증하는 워크로드를 처리하거나 재해 복구 기능을 제공한다. 매우 복잡한 구성에서는 일부 데이터가 두 환경 간을 수시로 이동하기도 한다. 예를 들어 퍼블릭 클라우드의 고객 관계 애플리케이션(CRM)과 프라이빗 클라우드의 재무 애플리케이션 간에 데이터가 이동할 수 있다. 이러한 경우 전체 환경에 걸쳐 리소스를 관리하는 툴을 활용할 수 있다.



〔그림 1〕 신기술 하이프사이클〔참조 : 가트너 그룹〕



〔그림 2〕 하이브리드 클라우드

하이브리드 클라우드는 다음을 비롯하여 수많은 이점을 제공한다[1].

- 빠른 IT 환경 구축과 짧은 투자 회수 기간
- 최적화된 IT 리소스 활용 및 IT 비용 지출
- 장소에 구애받지 않는 애플리케이션, 데스크톱 및 정보 액세스
- 빠른 확장 또는 수요 변화에 따른 재할당
- 에너지, 인프라스트럭처 및 설비비용 절감
- IT 인력 및 기업 전반의 생산성 증진
- 보안 및 정보 자산의 보호 강화

Ⅱ. 하이브리드 클라우드 활용 기술

2.1. EMC 하이브리드 클라우드[1]

EMC는 오픈스택, 데이터 저장, 데이터 복구 기술 등을 가진 스타트업 3곳을 인수합병 했다.

1) **클라우드 스케일링(cloudscaling)** : 오픈소스인 '오픈스택' 기반으로 IaaS 제공하는 업체이며 프라이빗 클라우드나 하이브리드 클라우드를 구축할 때 해당 기술을 사용한다. 핵심 제품으로는 오픈 클라우드 시스템(Open Cloud System, OCS)이 있는데 이는 클라우드에서 컴퓨팅, 스토리지, 네트워킹 기술을 관리할 수 있게 도와준다. 특히 클라우드 기반 애플리케이션을 효율적으로 관리하도록 돕고 있다.

2) **매지내틱스(Maginatics)** : 클라우드 스토리지 플랫폼을 제공하는 업체이며 모바일 등에서 얻은 대용량 데이터를 관리하고 데이터 보안 기술을 연구하고 있다. 예를 들어 여러 클라우드 저장소에 데이터를 복제하거나 WAN 최적화 기술을 제공한다. 대형 오브젝트 스토리지를 관리하거나 멀티쓰레드 기술도 지원하고 있다.

3) **스패닝(SPANNING)** : 클라우드 애플리케이션에 저장된 데이터를 백업·복구하는 기술을 개발하고 있다. 구글앱스, 세일즈포스닷컴, 'MS 오피스 365' 등에 사용되던 데이터들을 옮기고 보호하는 기술을 제공하고 있다.

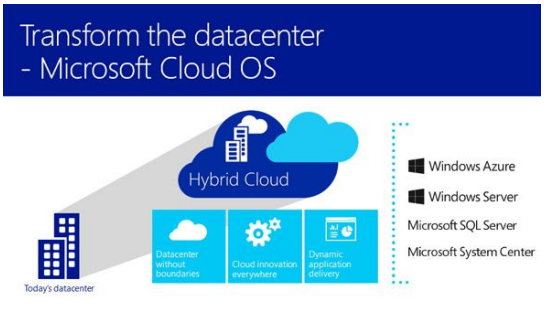
2.2. Microsoft 하이브리드 클라우드[2]

2.2.1. 클라우드 OS

마이크로소프트 클라우드 OS는 프라이빗, 퍼블릭 클라우드라는 틀에 머물러 제한적으로 IT 자원을 사용하는 것이 아니라 그 경계를 허물어 리소스를 활용하는 하이브리드 클라우드를 제공한다는 점이 가장 큰 특징이다. (그림 3)은 마이크로소프트의 윈도우 서버와 윈도우 시스템센터로 구축된 프라이빗 클라우드를 넘어 윈도우 애저가 제공하는 퍼블릭 클라우드 서비스 및 마이크로소프트 파트너사의 클라우드까지 하나로 연계되어 단일화된 체계로 하이브리드 클라우드 환경을 운영할 수 있음을 보여주고 있다.

더불어, 클라우드 OS는 통합된 클라우드 플랫폼으로서의 환경을 제공함에 따라 실제 업무 현장에서 데이터센터를 혁신하고 데이터의 크기, 형태를 아울러 통합 관리, 분석을 통해 진정한 통찰력을 제공하며 IT 소비자화를 실현하고 이를 통해 최신 응용 프로그램을 구현시킬 수 있는 환경을 제공한다.

이러한 하이브리드 클라우드 환경은 시장 변화에 빠르게 대응할 수 있는 경쟁력을 갖추는데 핵심적인 역할을 한다. 예를 들어 개발자의 경우, 단 한 번의 코드 작성으로 윈도우 서버와 윈도우 시스템 센터로 구축된 기업 내 클라우드와 파트너 클라우드, 그리고 윈도우 애저의 서비스까지 아울러 변경 사항을 배포 및 적용할 수 있다.



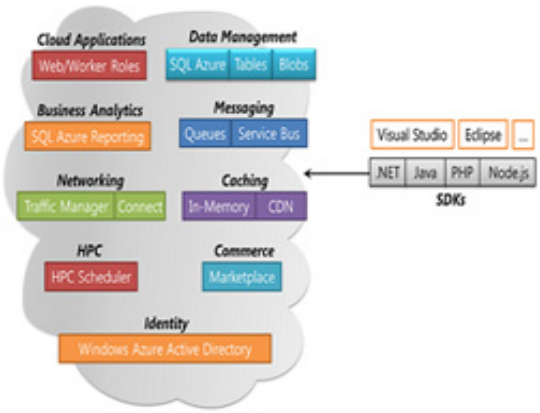
〔그림 3〕 마이크로소프트 클라우드 OS 시스템

2.2.2. 윈도우 애저[3]

Windows Azure란 퍼블릭 클라우드에 대한 마이크로소프트의 플랫폼이다. 사실 Azure란 단어가 공식 명칭에서 제외할 것으로 보이기에 앞으로는 공식호칭이 Windows Cloud가 될 것으로 예상된다.

2.2.2.1. Windows Azure 구성요소

Windows Azure가 무엇을 제공하는지 살펴보려면 Azure의 서비스들을 각각의 카테고리별로 그룹지어 보는 것이 좋다. (그림 4)는 카테고리별로 나누어 놓은 모습을 보여주고 있다.



〔그림 4〕 Windows Azure의 다양한 클라우드 서비스〔4〕

2.2.2.2. 클라우드 응용 프로그램

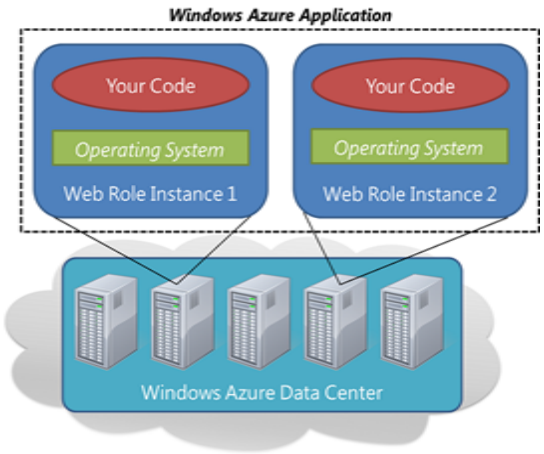
Windows Azure 응용 프로그램은 프로그램 개발자들의 데이터 센터에서 동작하는 응용 프로그램과 거의 유사하다. 하지만 Windows Azure는 신뢰도가 높고 프로그램 확장성이 높아서 기존의 응용 프로그램을 만들 때 도움을 주도록 설계되어 있기 때문에 Windows Azure의 응용 프로그램을 만드는 것은 기존의 응용 프로그램을 만드는 것과는 약간에 차이가 있다.

Azure에서는 모든 응용 프로그램이 하나 이상의 Role(역할)로 구현되어야 한다. 현재 Azure는 두 가지 유형의 Role을 제공하고 있다. Web Role(웹 역할)과 Worker Role(작업자 역할)이다. Web Role은 웹 브라우저나 기타 HTTP 클라이언트와 직접적으로 상호작용하는 코드(이 코드는 주로 마이크로소프트의 웹 서버인 IIS를 사용한다.)를 위해서 설계되었으며 Worker Role은 좀 더 일반적이고 다양한 코드들을 실행하기 위해서 만들어졌다.

수많은 데이터를 병렬로 처리하는 응용 프로그램을

작성해야 하는 경우에는 오로지 Worker Role만을 사용해야 한다. 응용 프로그램에 어떤 Role을 적용하던지 간에, 각 Role의 코드는 [Role 인스턴스] 안에서 실행된다. 실제로 Role 인스턴스라는 것은 윈도우 서버를 구동하고 있는 가상 머신(VM)이다. 이 VM은 Windows Azure 데이터 센터 안에서 운영되고 있다. (그림 5)는 두 개의 Web Role 인스턴스를 실행하는 응용 프로그램이 데이터센터 안에 놓여져 있는 모습을 보여주고 있다.

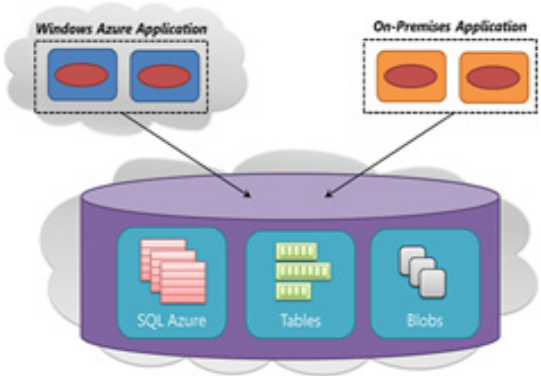
위와 같은 경우, 각각의 Web Role 인스턴스는 동일한 윈도우 서버 상에서 동일한 응용 프로그램 코드의 복사본을 실행할 것이다. 그리고 Windows Azure는 자동으로 로드 밸런싱(load balance, 부하 균형)을 수행하여 모든 사용자의 요청을 두 개의 인스턴스로 균등하게 배분한다.



〔그림 5〕 두 개의 Web Role 인스턴스를 실행〔5〕

2.2.2.3. 데이터 관리

모든 각각의 Windows Azure 응용 프로그램은 하나 이상의 Role 인스턴스 안에서 실행된다. 즉, 하나 이상의 VM 안에서 실행된다는 것이다. 그리고 각각의 VM은 응용 프로그램이 자유롭게 사용할 수 있는 로컬 저장소(하드 드라이브 등)를 가지고 있다. 하지만, 로컬에 파일이나 데이터를 저장하는 행동은 하지 않아야 한다. Windows Azure는 관리상의 이유로 주기적으로 인스턴스들을 종료하고 바꾸기 때문에 로컬 저장소에 놓아 둔 데이터는 아무런 예고도 없이 사라져 버릴 수 있다. 그렇기 때문에 응용 프로그램이 영구적으로 저장해야 하는 데이터들은 반드시 VM 외부에 저장되어야만 한다.



〔그림 6〕 Windows Azure의 데이터 관리 옵션〔6〕

이를 위해서 Windows Azure는 (그림 6)에서 보이는 것과 같이 3가지 종류의 데이터 관리옵션을 제공하고 있다.

각각의 옵션은 저마다의 쓰임새가 있다. 하나는 관계형 스토리지이고, 다른 하나는 초고속으로 접근하는 단순한 형식의 데이터 저장소(대용량 지원)이고, 남은 하나는 자유로운 형식의 blob 스토리지이다. 이 3가지 중 그 어느 것을 사용하면 데이터는 Windows Azure 데이터센터 안에 있는 서로 다른 3개의 컴퓨터에 자동으로 복제된다. (그림 6)에서 보이는 것과 같이, 이 3가지 옵션은 Windows Azure 응용 프로그램에서도 접근이 가능할 뿐만 아니라 집에 있는 노트북, 핸드폰에서 실행되는 응용 프로그램에서도 접근이 가능하다. 하지만 이 3가지 옵션을 사용하게 되면 사용한 Azure 데이터 관리 서비스에 대해서 사용한 만큼 비용을 지불해야 하며 저장되어 있는 데이터에 대해서도 기가 단위로 월별 비용을 지불해야 한다는 단점이 있다.

1) SQL Azure

SQL Azure는 클라우드 기반의 SQL 서버라고 생각하면 된다. 관계형 데이터베이스 관리 시스템 즉, RDBMS의 핵심적인 기능을 모두 제공하고 있다. 예를 들면, 트랜잭션 관리를 제공하고, 다중 사용자의 동시 데이터 접근(데이터 무결성 보장)을 지원하며, ANSI SQL을 통해 질의할 수도 있게 한다. SQL Azure는 엔티티 프레임워크, ADO.NET, JDBC를 이용한 Java 및 그 밖의 다양한 데이터 접근 기술을 사용하여 연결할 수 있다. 사용자들은 SQL 서버를 대상으로 작업했던 것과 거의 똑같은 방식으로 사용할 수 있다. 그리고 대부분의

T-SQL 언어를 지원할 뿐만 아니라 SSMS(SQL Server Management Studio) 도구나 SQL Server 데이터 도구들을 사용하여 접근할 수도 있기 때문에 이미 SQL 서버에 익숙한 사람들이거나 SQL 서버가 아닌 그 밖의 관계형 데이터베이스에 익숙한 사람이라도 RDBMS를 다룰 줄 안다면 SQL Azure를 사용하는 것은 매우 쉽다.

2) Table

수백 기가로 단순한 형식 데이터에 빠르게 접근할 필요가 있는 Windows Azure 응용 프로그램을 만들고자 한다면 그러한 데이터에 대해 복잡한 SQL 질의를 수행할 필요는 없다. 또한 관계형 저장소를 제공하지 않기 때문에 Table을 사용하는 응용 프로그램은 string, integer, date 등 다양한 형식의 속성들을 저장할 수 있다. 그런 다음에 응용 프로그램은 특정 그룹에 대한 고유 키를 제공하여 속성들의 그룹을 가져올 수 있다. 조인과 같은 복잡한 작업은 지원되지 않지만 Table은 형식 데이터에 빠르게 접근할 수 있다는 장점이 있다. 더불어, 단일 테이블이 테라 바이트 규모의 데이터를 담을 수 있으며, 확장성도 대단히 높다. 그리고 그러한 단순함에 걸맞게 Table은 일반적으로 SQL Azure의 관계형 저장소를 사용하는 것보다는 비용이 저렴하다.

3) Blob

Blob는 구조적이지 않은 자유 형식의 이진 데이터를 저장하기 위해서 고안되었다. Table과 마찬가지로 비용이 저렴할 뿐만 아니라 단일 Blob의 용량은 테라 바이트만큼 커질 수도 있다. 예를 들면 동영상을 저장하는 응용 프로그램 혹은 데이터를 백업하거나 기타 이진 정보를 저장하는 응용 프로그램이라면 간단하고 저렴한 스토리지인 Blob을 사용하는 것이 좋을 것이다. Windows Azure 응용 프로그램은 또한 Windows Azure 드라이브도 이용할 수 있다. 이 드라이브는 Blob를 통해서 Azure 인스턴스 안에 설치된 윈도우 파일 시스템에 영구적인 저장소를 제공할 수 있게 한다.

2.2.2.4. 비즈니스 분석

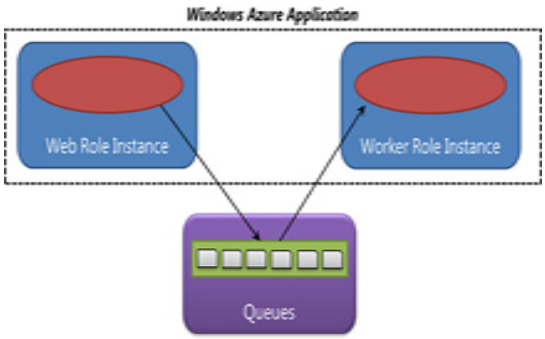
저장된 데이터를 사용하는 가장 보편적인 방법 중 하나는 그러한 데이터를 기반으로 보고서를 만드는 것이다. Windows Azure는 SQL Azure 안에 있는 관계형 데이터를 가지고 보고서를 만들 수 있도록 SQL Azure 리포팅을 제공하고 있다. SQL 서버에서 제공되는 리포팅 서비스의 서브셋인 SQL Azure 리포팅은 Windows Azure 응용 프로그램에서 리포팅을 만들 수 있게 한다. 리포트는 HTML, XML, PDF, Excel 등 다양한 포맷으로 생성할 수 있으며, 응용 프로그램 안에 삽입되거나, 웹 브라우저를 통해서 보여질 수 있다. SQL Azure 데이터를 분석하는 또 다른 방법으로는 비즈니스 인텔리전스 도구를 사용하는 것이다. 클라이언트 입장에서는 SQL Azure나 SQL 서버나 크게 다를 바가 없다. 그렇기에 비즈니스 인텔리전스 도구는 SQL Azure를 대상으로도 잘 동작한다.

2.2.2.5. 메시징(Messaging)

어떤 작업을 수행한 결과와 관계없이 코드는 종종 다른 코드와 통신을 해야 할 필요가 있다. 그렇게 하기 위한 일반적인 방법 중 하나는 큐를 사용하는 메시지(queued messaging)를 이용하는 것이다. 물론 다른 방법을 사용할 수도 있겠지만 별개의 응용 프로그램은 서로 다른 조건을 요구할 수 있기 때문에 Windows Azure는 그러한 통신을 위해 서로 다른 2가지의 기술 즉, 큐(Queues)와 서비스 버스(Service Bus)를 제공하고 있다.

1) Queue(큐)

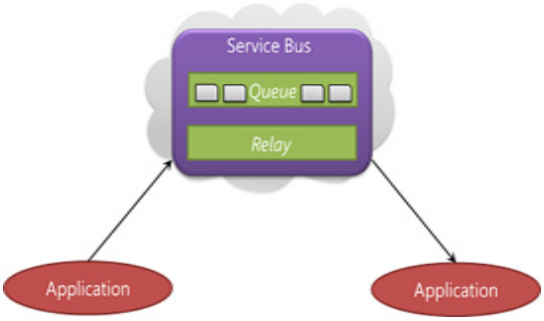
Windows Azure에 의해 제공되는 Queue 서비스는 이해하기가 쉽다. 말 그대로 큐 기능이다. 즉, 어떤 응용 프로그램이 메시지를 큐에 놓아두면 다른 응용 프로그램이 그것을 읽어가는 방식이다. 현재 Queue를 사용하기에 가장 적합한 곳은 (그림 7)에서 보이는 것과 같이 Web Role 인스턴스가 Worker Role 인스턴스와 통신하는 경우이다.



〔그림 7〕 Web Role 인스턴스가 큐를 통해서 Worker Role 인스턴스와 통신〔7〕

2) 서비스 버스(Service Bus)

Windows Azure는 서비스 버스도 지원하고 있다. 서비스 버스는 클라우드 안에서 소프트웨어를 연결하는 좀 더 일반적인 접근 방식이라고 볼 수 있다. 사실 서비스 버스도 내부적으로는 큐 서비스를 제공하고 있다. 하지만 이 큐 서비스가 앞서 설명한 메세징의Queue 서비스를 말하는 것은 아니다. 둘은 확연한 차이가 많다. 서비스 버스는 일반적으로 (그림 8)에서 보여지는 것과 같이 서로 다른 응용 프로그램을 연결하는 경우에 사용된다.



〔그림 8〕 서비스 버스는 큐를 통해서나 혹은 직접적으로 응용 프로그램 간에 통신〔8〕

2.3. Optenet 하이브리드 클라우드 보안 솔루션[9]

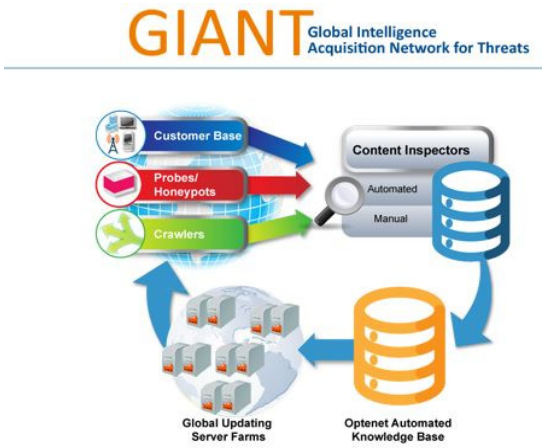
보안 경력이 10년 이상인 Optenet은 뛰어나게 진보된 기술로 IT 업계를 선도하고 있으며 대표적인 기술로는 Optenet MIDASTM와 Optenet GIANTTM이 있다. 이들은 특히 웹 2.0 보안위협으로부터 탁월하게 보호해 주며 고도의 정확성과 민첩성을 제공하고 있다.

2.3.1. Optenet GIANT™

Optenet GIANT(Global intelligence Acquisition Network for Threats)TM는 지속적으로 새로운 보안위협이 나타나면 그 위협요인을 확실하게 차단한다. 전 세계의 인터넷 소스로부터 정보들을 수신하여 모든 Optenet 솔루션 인스턴스에 업데이트를 추진하고 있다((그림 9) 참조).

2.3.2. Optenet MIDAS™

Optenet MIDAS (Multicontent inspection & Dynamic Analysis System)TM는 오프라인과 온라인을 통해 들어온 수많은 정보들 중에서 부적절한 불법 유해 콘텐츠를 신속정확하게 식별할 수 있다((그림 10) 참조).



〔그림 9〕 Optenet GIANT™ 기술

〔그림 10〕 Optenet MIDAS™ 기술

2.3.3. 집중감시, 관리, 보고 및 계층화된 행정

2.3.3.1. 실시간 모니터링

Optenet의 엔터프라이즈 솔루션의 모든 모니터링 은 사용가능한 시스템을 확인하기 위해 가장 빠르게 실시간으로 포착한다. 추가적인 라이센스 필요 없이 솔루션에 통합하여 데이터베이스에서 지원된 보고서는 기업의 요구에 맞게 사용자가 정의할 수 있다.

2.3.3.2. 중앙집중식 관리 및 분산운영

시스템은 부분적이고 간단하지만 내부의 중앙관리 콘

솔은 여러 위치에 있는 정책관리를 순조롭게 처리할 수 있다. 관리자는 세계적인 규모의 네트워크 인프라스트럭처를 통제하기 위해서 불필요한 정책을 제한하고 독립적으로 콘솔을 사용할 수 있다.

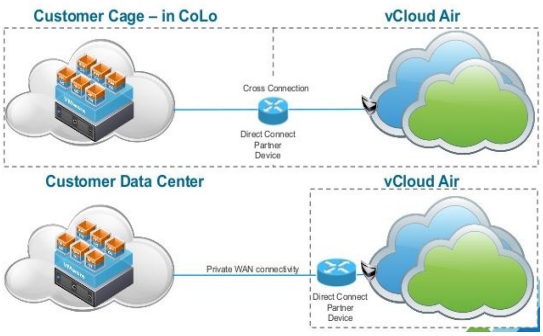
2.3.3.3. 효율적이고 효과적인 계층관리

관리자는 로컬 또는 글로벌, 구성 및 사용자, 그룹, 워크스테이션이나 네트워크에 의한 액세스 정책을 간단하고 효율적으로 정의할 수 있다. 이러한 방식으로 모든 위치에 대한 단계별 접근을 쉽게 허용할 수 있다. 그리고 로컬 관리자에게는 특정 요구사항에 따른 서로 다른 액세스 레벨을 제공하기 쉽다. 레이어 관리 시스템은 최대용량 저장소와 효율적인 업무, 기업을 보호할 수 있는 안전망을 제공한다.

2.4. V 클라우드[10]

2.4.1. V 클라우드 정의

VMware vCloud Air 혹은 VMware vCloud Air Network 서비스 공급업체 파트너사인 구글은 데이터 센터 및 애플리케이션을 클라우드로 원활하고 안전하게 확장할 수 있도록 하이브리드 클라우드 컴퓨팅에 관한 약속을 이행하고 있다. 상호 간에 신뢰할 수 있는 VMware 기술 기반으로 구축된 클라우드 서비스를 통해 새로운 워크로드를 프로비저닝하거나 사내 데이터 센터 또는 사내 프라이빗 클라우드 간의 기존 워크로드를 퍼블릭 클라우드로 이동하고 필요한 경우에는 다시 원래대로 이동하여 진정한 하이브리드 클라우드를 만들 수 있다. VMware vCloud Air 혹은 vCloud Air Network는 여러 지역의 다른 클라우드 공급업체에서도 V 클라우드 서비스 네트워크를 사용할 수 있도록 하여 고객들에게 유연한 모바일 환경을 제공한다((그림 11) 참조).



〔그림 11〕 V 클라우드

2.4.2. V 클라우드의 이점

V 클라우드 서비스에서 지금과 동일한 방식으로 애플리케이션을 작성, 구축 및 관리할 수 있으며 보편화된 플랫폼을 바탕으로 구축된 VMware 인프라스트럭처에서 현재 보안시스템을 강화할 수 있다. 통합형 하이브리드 인프라스트럭처(데이터 센터와 퍼블릭 클라우드)를 " 단일 창" 관리 프레임워크에서 관리할 수 있다. 또한 이미 가지고 있는 툴박스, 프로세스 및 기술 등을 사용할 수 있다.

기존의 워크로드와 새로운 워크로드를 클라우드에 신속하게 구축하고 요구사항의 변경에 따라 기업 내부 및 외부 환경 간에 네트워크를 유연하게 이동할 수 있다. VMware 또는 vCloud Air Network 서비스 공급업체는 에코시스템을 통해 향상된 클라우드 서비스를 전 세계에서 사용하고 선택할 수 있다. 기업들은 102개 국가의 로컬 vCloud Air 데이터 센터와 vCloud Air Network 서비스 공급업체를 통해서 독립적으로 데이터를 관리하여 사유 안정성이 보장된다.

2.5. 기업 적용사례

앞에서 설명한 사례를 포함하여 다음과 같은 기업 적용사례가 있다.

1) EMC, 스타트업 3곳 인수합병 및 하이브리드 클라우드 강화
2) EMC "클라우드·빅데이터 통합"
3) IBM은 서비스로써 소프트웨어의 인터넷 클라우드 서비스와 Bluemix을 확장[11]
4) OpenStack은 IBM Bluemix를 사용하여 확장성 스위프트 응용 프로그램을 신속하게 구축하고 배포[12]
5) 일반적으로 사용가능한 현재 IBM의 Bluemix[13]
6) GameStop Bluemix와 새로운 클라우드 앱 개발[14]
7) VM웨어·구글, 하이브리드 클라우드 시장 공략 맞

손[15]

Ⅲ. 클라우드 컴퓨팅 보안

최근 수년간 [표 2]와 같이 클라우드 환경에서의 다양한 사고가 발생했음을 알 수 있다. 사고원인은 주로 H/W 시스템 오류, 천재지변, 관리실수에서 해킹에 의한 것이며, 피해유형으로는 일시적인 서비스 장애, 데이터 유출/손실 등의 피해가 발생하였음을 알 수 있다.

[표 2]에서 보듯이 클라우드 컴퓨팅의 실현을 위해서는 보안적인 문제점 해결이 선결과제이다. 이를 위하여 가트너 그룹과 유럽의 ENISA, CSA(Cloud Security Alliance) 등에서 활발한 연구가 진행중이다[16].

〔표 2〕 클라우드 관련 주요 보안사고 현황(참조 : KISA 자료)

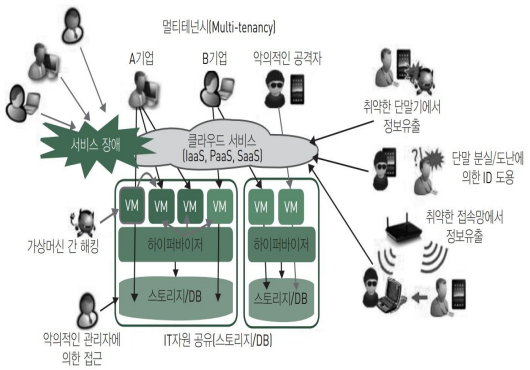
연도	장애원인	유형	회사	주요 내용
2006	HW·시스템 오류	서비스 장애	아마존	인증요청의 쇄도로 인한 인증서버 다운
	관리 부주의	데이터 손실	미디어 맥스	폐업으로 인한 2만명의 데이터 손실
2009	HW·시스템 오류	서비스 장애	세일즈 포스	네트워크 장비와 메모리 배치 에러로 1시간 서비스 중단
		서비스 장애	이베이	페이글 지불결제 시스템 에러로 서비스 2시간 중단
		서비스 장애	구글	Gmail 2시간 서비스 장애 반복 발생
		서비스 장애	MS	스마트폰 서비스 사이드의 서비스 중단
	관리 부주의	서비스 장애	구글	구글 앱스 관리상 오류로 24시간 중단
2010	관리 부주의	데이터 유출	MS	BPOS 서비스 환경설정 오류로 인해 기업정보가 유출
2011	HW·시스템 오류	데이터 손실	구글	50만명 이용자의 메일내용 및 주소록이 삭제
		서비스 장애	아마존	아마존 EC2 백업 오류로 190여개 서비스 11시간 마비
		서비스 장애	애플	모바일이 마이그레이션에 따른 서버 과부하로 인한 마이클라우드 접속 불가
	천재지변	서비스 장애	구글	일본 대지진의 영향으로 해저케이블 손상 서비스 장애(Gmail, 안드로이드 마켓 등 서버 접속지연)
		서비스 장애	아마존	벼락으로 인한 정전사고로 아마존 EC2 장애
	해킹	서비스 장애	후지쯔	후지쯔 클라우드 서비스 DoS 공격받아 장애발생
	해킹	정보 유출	소니 PSN	7700만명의 이용자 정보 및 계좌 정보 유출
2012	HW·시스템 오류	서비스 장애	KT	uCloud 서버 스위치 오동작, 스토리지 오작동으로 인한 서비스 장애
		서비스 장애	세일즈 포스	스토리지 저장 실패로 인한 NA2 서비스 중단
	관리 부주의	데이터 손실	First Server	시스템 업그레이드 중 오류발생, 5천698개 회사의 데이터 손실
2013	천재지변	서비스 장애	아마존	폭풍우로 인한 정전사고로 아마존 EC2 장애(인스타그램, 넷플릭스, 핀터레스트, 헤로쿠 등의 서비스가 중단)
	해킹	데이터 손실	애플	해커(취약점 : 나의 맥북 찾기)에 의한 개인 정보의 삭제
	해킹	정보 유출	야후	45만명의 이용자 정보 유출
	해킹	정보 유출	Dropbo	직원 계정에 있던 사용자 이메일 명단이 유출되어, 해당 사용자들에게 스팸메일 발송
	해킹	정보 유출	어도비(Adobe)	어도비(Adobe)의 서버가 해킹돼어 290만명의 개인정보와 어도비 아크로뱃(Acrobat), 콜드퓨전(ColdFusion), 콜드퓨전빌더(Cold Fusion Builder) 등의 소프트웨어 소스 코드 일부 유출
	해킹	정보 유출	에버노트	메모/정보 정리 툴 제공 클라우드 대표 서비스인 Evernote에서 사용자명, 전자메일주소, 암호화된 패스워드 유출
2014	해킹	서비스 장애	영국 Code Spaces	AWS를 사용하여 호스팅 서비스를 제공하던 중에 DDoS 공격으로 모든 자원을 지움

3.1. 클라우드 컴퓨팅 환경의 보안 위협[17]

클라우드 컴퓨팅은 사용자가 프로그램을 PC에 설치할 필요 없이 인터넷 환경만 구축되어 있다면 언제든 원하는 서비스를 이용할 수 있는 이점들이 있다.

- 데이터가 온라인상에 위치, 여러 기기들과 연동의 조화
- 소프트웨어를 각 기기마다 설치할 필요가 없기 때문에 비용절감
- 개인이 가지고 다녀야 하는 저장공간의 제약이 사라지므로 이동성과 휴대성이 용이
- 클라우드 컴퓨팅을 통해 일치된 사용자 환경을 구현

그러나 서버가 공격 받으면 개인 정보의 유출이 우려된다는 점이 있다. 기존 IT 환경의 보안 위협을 그대로 상속하고 클라우드 특성에 따른 가상화, 다중임차(Multi-tenancy), 원격지에 정보 위탁 · 사업자 종속, 모바일 기기 접속, 데이터 국외이전, 침해사고 대형화, 데이터센터의 안전성 등의 신규 공격 위협이 여전히 존재하고 있다. 또한 클라우드 컴퓨팅 환경 위협 공격에 대해 기존 보안 기술은 가상화의 구조적 특성 인식 한계, 하이퍼바이저 루트킷 등 진화하는 악성코드 탐지 한계, 빈번한 자원변동 및 물리자원 공유 특성으로 인한 가상머신의 보안관리 어려움이 존재한다. 이러한 문제들은 클라우드 컴퓨팅 서비스를 위협하는 가장 심각한 문제



〔그림 12〕 클라우드 컴퓨팅의 유형별 보안위협 개념도〔16〕

가 되고 있다((그림 12),[표 3] 참조).

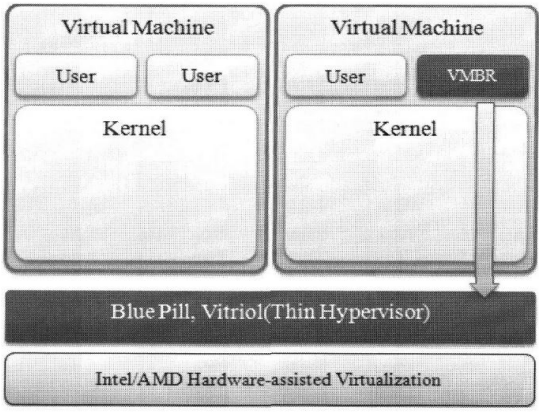
특히 클라우드 환경에서 이용되는 물리 자원들은 가상화 기술을 이용하여 클라우드 서비스 이용자들에게 효과적으로 보급된다. 공유 물리 자원들은 기본적으로 클라우드 환경에 맞도록 설계되어 있지 않아 하이퍼바이저가 자원 배분 역할을 수행하게 된다. 하지만 하이퍼바이저는 취약점이 많아 보안 위협에 노출될 수 있다.

〔표 3〕 CSA에서 발표한 클라우드 컴퓨팅 7대 위협

1. 클라우드 컴퓨팅 남용 및 불손한 사용(Abuse and Nefarious Use of Cloud Computing) - 악의적인 의도를 가진 사람들이 클라우드를 도입하게 되면, 모든 정보가 가상에 있게 되기 때문에 기존의 봇넷보다 더 찾아내기 힘들고 위험한 존재가 될 수 있다.
2. 안전하지 않은 애플리케이션 프로그래밍 인터페이스(Insecure Application Programming) - 애플리케이션 구축을 서두르기 위해서 기존의 코드를 재사용하거나 합성해서 사용하면 보안에 구멍이 뚫리기 마련이다.
3. 악의를 가지고 있는 내부 관계자(Malicious Insiders) - 클라우드 컴퓨팅이 갑자기 떠오르면서, 관련 경험을 가진 사람을 급하게 채용하면 도덕적으로 적합하지 않는 사람을 고용할 가능성도 높아지게 된다.
4. 공유 기술에 취약점(Shared Technology Vulnerabilities) - 가상머신을 적절히 관리하지 못하면, 하나의 작은 실수로 전체가 다 위협받을 수 있다.
5. 데이터 유실 및 유출(Data Loss and Leakage) - 데이터를 보호하기 위한 기존의 제어는 새로운 클라우드 환경에서 적합하지 않을 수 있으며, 감시하기가 더 힘들다.
6. 계정, 서비스 및 트래픽 하이재킹(Account, Service & Traffic Hijacking) - 이미 각종 악성 사이트로 유도(redirected)하는데 사용된 많은 하이재킹(Hijacking) 기법에 취약하다.
7. 공개되지 않은 위협 프로파일(Unknown Risk Profile) - 서비스 제공업체의 투명성이 떨어져 고객사가 시스템의 구성이나 소프트웨어 패치를 실행해야 하는지 알지 못할 때가 많다.

CSA(Cloud Security Alliance)에서 발표한 클라우드 컴퓨팅에서 발생 가능한 위협은 [표 3]과 같다.

(그림 13)은 가상화 기술을 이용한 루트킷인 VMBR(Virtual Machine Based Rootkit)의 기본 구조이다. 대표적인 VMBR로는 Subvirt, Blue Pill, Vitriol, CloudBurt 등이 있으며, 이러한 가상화 기반의 악성코드의 경우 루트킷 존재 여부를 탐지하기 어렵다. Subvirt은 VMware와 Virtual PC에서 운영체제에 악의적인 모듈 등록을 통하여 시스템 권한을 획득하는 기술이며 Blue Pill, Vitriol의 경우, Intel 및 AMD의 하드웨어 지원 가상화 기술을 이용하여 VM-root 권한을 획득하는 기술이다.



〔그림 13〕 VMBR의 기본구조〔18〕

3.2. 클라우드 보안 관련 국내·외 정책 동향

3.2.1. 미국 FedRAMP[19]

미국은 클라우드 제품의 위험관리를 위한 FedRAMP 프로그램을 만들어 운영 중에 있다.

FedRAMP 관련 문서는 15개 이상의 정부기관 담당자로 구성되어 있는 GSA 산하 클라우드 컴퓨팅 보안 작업그룹에서 작성하였으며, NIST 및 연방 CIO 협의회와 협력하여 FedRAMP 문서를 보강하였다. 특히 정부기관에 도입된 클라우딩 컴퓨터 시스템에 대한 모니터링 프레임워크를 개발하는데 있어 NIST 및 NSA와

〔표 4〕 FedRAMP 작업 경과

시기	주요내용
2010.3	GSA, FedRAMP 도입 타당성 검토
2010.11	미국 정부기관 클라우드 제품 및 서비스 보안성 인증심사 및 승인에 관한 보고서 발표
2010.12.8	OMB CIO Memorandum 발표
2011.11.2	미국 정부기관용 클라우드 컴퓨팅 보안성 인증심사 프레임워크 발표
2011.12.8	CIO, FedRAMP 정책지침 발표
2012.1.8	FedRAMP JAB, FedRAMP 기본 통제항목 발표
2012.2.8	GSA, FedRAMP 인증지침 발표
2012.6.6	FedRAMP 제도 시행

긴밀하게 협조체계를 유지하였다.

FedRAMP(Federal Risk and Authorization Management Program)는 미국정부와 여러 부서 및 기관으로 구성된 차원의 프로그램으로서 미국방부, GSA의 CIO위원회들이 의사결정을 한다. 이들은 정부 및 클라우드 서비스 제공 업체 사이의 투명성을 강화하기 위해 보안 인증 패키지를 활용한다. 그리고 클라우드 보안 평가의 신뢰도를 향상시키려고 지속적인 모니터링 자동화를 추진 중이다. 또한 미국정부가 보안수행평가를 수행하는 데 필요한 비용과 시간, 자원을 절약할 수 있는 이점을 지니고 있다.

FedRAMP는 절차는 [표 5]와 같이 3단계로 구성된다.

보안성 인증심사에서 확인하는 주요 내용은 (그림 14)와 같다.

〔표 5〕 FedRAMP Process

단계(process)	주요내용
보안성 인증심사 (Security Assessment)	NIST 800-53 보안통제 기본항목 (중간 등급 이하)을 기반으로 FISMA에 따라 구성한 표준 요구사항(인증기준)에 적합한지 여부를 심사하는 과정
인증제품/서비스 도입 (Leveraging and Authorization)	연방 정부기관이 FISMA에 따라 민간 클라우드 컴퓨팅 제품/서비스를 도입할 때 실시해야 하는 보안성 검토과정을 FedRAMP 인증심사 결과물을 검토하는 것으로 대신하여 도입하는 과정
인증 사후관리 (Ongoing Assessment & Authorization)	클라우드 인증 제품/서비스가 미국 정부기관에 도입된 이후, 인증효력 유지를 위해 사후 및 갱신 심사를 진행하는 과정

ID	Family	Low	Moderate
AC	Access Control	11	18 (25)
AT	Awareness and Training	4	4 (1)
AU	Audit and Accountability	10	11 (8)
CA	Certification, Accreditation, and Security Assessment	7 (1)	8 (7)
CM	Configuration Management	8	11 (15)
CP	Contingency Planning	6	9 (15)
IA	Identification and Authentication	7 (8)	8 (19)
IR	Incident Response	7	9 (9)
MA	Maintenance	4	6 (5)
MP	Media Protection	4	7 (3)
PE	Physical and Environmental Protection	10	16 (4)
PL	Planning	3	4 (2)
PS	Personnel Security	8	8 (1)
RA	Risk Assessment	4	4 (6)
SA	System and Services Acquisition	6 (1)	9 (13)
SC	System and Communications Protection	10	20 (12)
SI	System and Information Integrity	6	12 (16)
	Totals (Controls and Enhancements):	125	325

〔그림 14〕 FedRAMP SSP에서 정의된 보안 통제 항목

3.2.2. 유럽

유럽의 ENISA(European Network and Information Security Agency)에서는 클라우드 컴퓨팅의 위협요소와 관련하여 정책/조직 위험, 기술적 위험, 법적위험, 클라우드에 특화되지 않은 위험, 이렇게 4가지 영역으로 분류하고 세부적으로는 관리부재, 규제 준수, 서비스 제공자에 의존하는 현상, 관리 인터페이스의 보완, 데이터 보호, 악의적 내부자 등의 35개 항목으로 구분하여 사례 분석 및 위험을 평가하는 절차를 만들었다. 또한 클라우드에 특화된 취약점과 자산을 분류하고 12개의 정보보증 요구사항을 제시하였다.

〔표 6〕 POLICY AND ORGANIZATIONAL RISKS

절차(PROCEDURE)	위험(RISK)
LOCK-IN	HIGH
LOSS OF GOVERNANCE	HIGH
COMPLIANCE CHALLENGES	HIGH
LOSS OF BUSINESS REPUTATION DUE TO CO-TENANT ACTIVITIES	MEDIUM
CLOUD SERVICE TERMINATION OR FAILURE	MEDIUM
CLOUD PROVIDER ACQUISITION	MEDIUM
RESOURCE EXHAUSTION (UNDER OR OVER PROVISIONING)	MEDIUM
ISOLATION FAILURE	HIGH
CLOUD PROVIDER MALICIOUS INSIDER - ABUSE OF HIGH PRIVILEGE ROLES	HIGH
MANAGEMENT INTERFACE COMPROMISE (MANIPULATION, AVAILABILITY OF INFRASTRUCTURE)	MEDIUM
INTERCEPTING DATA IN TRANSIT	MEDIUM
DATA LEAKAGE ON UP/DOWNLOAD, INTRA-CLOUD	MEDIUM
INSECURE OR INEFFECTIVE DELETION OF DATA	MEDIUM
DISTRIBUTED DENIAL OF SERVICE (DDOS)	MEDIUM
ECONOMIC DENIAL OF SERVICE (EDOS)	MEDIUM
LOSS OF ENCRYPTION KEYS	MEDIUM

절차(PROCEDURE)	위험(RISK)
UNDERTAKING MALICIOUS PROBES OR SCANS	MEDIUM
COMPROMISE SERVICE ENGINE	MEDIUM
CONFLICTS BETWEEN CUSTOMER HARDENING PROCEDURES AND CLOUD ENVIRONMENT	MEDIUM
SUBPOENA AND E-DISCOVERY	HIGH
RISK FROM CHANGES OF JURISDICTION	HIGH
DATA PROTECTION RISKS	HIGH
LICENSING RISKS	MEDIUM
NETWORK BREAKS	MEDIUM
NETWORK MANAGEMENT (IE. NETWORK CONGESTION / MIS-CONNECTION / NON-OPTIMAL USE)	HIGH
MODIFYING NETWORK TRAFFIC	MEDIUM
PRIVILEGE ESCALATION	MEDIUM
SOCIAL ENGINEERING ATTACKS (IE. IMPERSONATION)	MEDIUM
LOSS OR COMPROMISE OF OPERATIONAL LOGS	MEDIUM
LOSS OR COMPROMISE OF SECURITY LOGS (MANIPULATION OF FORENSIC INVESTIGATION)	MEDIUM
BACKUPS LOST, STOLEN	MEDIUM
UNAUTHORIZED ACCESS TO PREMISES (INCLUDING PHYSICAL ACCESS TO MACHINES AND OTHER FACILITIES)	MEDIUM
THEFT OF COMPUTER EQUIPMENT	MEDIUM
NATURAL DISASTERS	MEDIUM

〔표 7〕 정보보증 요구사항

PERSONNEL SECURITY
SUPPLY-CHAIN ASSURANCE
OPERATIONAL SECURITY
IDENTITY AND ACCESS MANAGEMENT
ASSET MANAGEMENT
DATA AND SERVICES PORTABILITY
BUSINESS CONTINUITY MANAGEMENT
PHYSICAL SECURITY
ENVIRONMENTAL CONTROLS
LEGAL REQUIREMENTS
LEGAL RECOMMENDATIONS
LEGAL RECOMMENDATIONS TO THE EUROPEAN COMMISSION

3.2.3. 중국[21]

중국의 클라우드 서비스 시장 규모가 2020년까지 연평균 40.5%의 성장률을 기록할 것으로 예상되며 인터넷 서비스 업체, 통신 사업자, 데이터 센터 업체, 소프트웨어 서비스 업체 등 다양한 사업자들이 시장에서 경쟁하고 있다. 중국정부는 클라우드 컴퓨팅 기술을 보편화하고 국제 경쟁력을 갖춘 핵심 기업을 육성할 것을 목표로 하고 있다. 이와 다르게 중국 정부의 집중적인 견제와 규제로 인해 현지 업체들 간의 경쟁은 활성화되고 있으나, Microsoft, Amazon, IBM, Google 등 글로벌 업체들의 중국 내 비즈니스 전개는 부진한 상황이다.

닝샤(Ningxia)省의 경우, 지방 정부가 동 지역 내 대규모 데이터 센터 건립을 위한 AWS(Amazon Web Service) 파일럿 프로젝트를 승인하고 전자정부 서비스를 위해 Amazon의 플랫폼을 사용하기로 했으나, 중앙 정부는 여전히 자국 기업들의 IT 제품과 서비스를 우대하고 있는 실정이다.

아이러니하게도 중국경제시장이 성장할수록 사이버범죄도 증가하고 있다. 중국은 입법안을 수정해 사이버범죄에 대처하고 있다.

3.2.4 국내

클라우드 컴퓨팅 발전법이 국회통과('15.3) 후 금년 9월부터 시행됨에 따라 미래부, 행정자치부 등 관련기관이 클라우드 생태계 조성을 위한 대책들을 발표하였다.

금년 5월 10일 미래부는 '2015 클라우드 서비스(SaaS) 지원 사업' 발표하였으며, SaaS 개발이 가능한 국내 중소 SW 및 IT 기업을 대상으로 기업형(B2B)과 일반형(B2C)으로 나눠 연간 총 10억 원 내외의 개발비를 지원하고 있다.

또한 미래부와 행자부는 국가보안기술연구소, KISA, NIA 등 관련기관과 'FedRamp'와 같은 인증 제도를 한국 상황에 맞게 적용하는 방안을 개발 중에 있다. 공공기관이 민간 클라우드 서비스를 사용하기 위해선 보안이 가장 먼저 해결돼야 하기 때문이다. 하지만 보안인증제도인 한국판 페드램프(K-FedRAMP)는 내년에나 선보일 것으로 예상된다. 필요하다는 판단 때문이다. 이를 통해 클라우드 서비스 업무 및 정보의 중요도에 따라 보안 등급을 구분하고 등급별 인증기준 개발, 운영지침 수립, 시범적용을 통한 클라우드 보안인증제도의 도입에 활용한다는 방침이다.[22]

특히 KISA는 이번 사업을 통해 클라우드 보안등급 및 인증기준을 개발하고 클라우드 보안인증 운영 방안을 마련한다는 방침이다. 또 보안인증 시범 적용을 통해 다양한 산업에서 이를 활용할 수 있는 기초를 마련할 계획이다.

여기에는 국제 표준인 미 페드램프(FedRAMP, 연방정부 클라우드 보안통제 항목), ISO/IEC 27001(정보보호 관리체계 기준), 27017(클라우드 서비스 제공자를 위한 개인정보보호 지침), 27018(클라우드 서비스 제공자를 위한 정보보호 지침) 등을 적극 참고할 예정이다.

한국인터넷진흥원(KISA)은 금년 7월부터 '클라우드 보안 등급별 인증기준 개발 및 시범적용' 사업을 시행하고 있다. 6개월간 시행되는 이번 사업은 클라우드 서비스 제공자의 보안수준 향상과 침해사고에 대한 피해를 최소

〔표 8〕 클라우드 서비스 인증제

측정목적	측정내용	측정수	정점수
가용성	신청기관은 클라우드 서비스를 약정된 내용에 따라 상시적으로 제공하기 위해 제반 조치를 하여야 한다.	5	14
확장성	클라우드 서비스 제공자는 클라우드 서비스 수요에 유연하게 자원을 확장하여 제공할 수 있도록 필요한 정책, 인적 물적 자원을 갖추어야 한다.	5	12
성능	클라우드 서비스 제공자는 서비스의 품질(속도)을 보장하기 위해 적절한 성능을 유지하여야 한다. 이를 위해 필요한 정책, 인적 물적 자원 등을 갖추어야 한다.	6	13
데이터 관리	클라우드 서비스 제공자는 클라우드 서비스 이용자의 데이터를 안전하게 보호/관리하기 위해 필요한 정책 및 인적, 물적 자원 등을 갖추어야 한다.	5	15
보안	조직의 보안을 효과적으로 구현하기 위해 관리체계를 수립하여야 한다. 또한 조직의 물리적 시설 및 설비를 보호하기 위해 물리적 보호 방안이 마련되어야 한다. 또한 다양한 취약성을 분석하고 그에 대한 적절한 대책을 마련하고 적용하여야 한다.	10	22
서비스 지속성	사용자가 믿고 클라우드 서비스를 이용할 수 있도록 사업자는 인적, 물적 기반을 확보하고 이를 관리하여야 한다.	4	13
서비스 지원	클라우드 서비스 제공자는 사용자의 서비스 만족도를 제고하기 위해 각종 기술지원, 제공방식의 다양성, 수준의 보장 등 지원 체계를 갖추어야 한다.	5	15
계		40	105

화하기 위해 클라우드 보안인증제도 도입이 필요하다는 판단 때문이다. 이를 통해 클라우드 서비스 업무 및 정보의 중요도에 따라 보안 등급을 구분하고 등급별 인증기준 개발, 운영지침 수립, 시범적용을 통한 클라우드 보안인증제도의 도입에 활용한다는 방침이다.

또한 한국클라우드서비스협회(KCSA)에서는 지난 2012년, '클라우드 서비스 인증제'를 시행하였다. [표 5]는 클라우드 서비스 제공업자를 평가하여 인증을 부여하는 제도를 의미한다. 이 제도의 목적은 클라우드 컴퓨팅의 확산과 경쟁력 강화에 있다.

Ⅳ. 결 론

IT시대에서 클라우드 기술이 상용화 되면서 프라이빗 클라우드와 퍼블릭 클라우드가 접목되는 하이브리드 클라우드 신기술이 국내외에서 새로운 화두로 떠오르고 있다. 하이브리드 클라우드는 기술성, 경제성, 효율성에서 많은 이점을 지니고 있다. 하지만 이에 대한 클라우드 컴퓨팅 서비스 보안대책을 마련해 반드시 운용해야만 할 것이다. 현재의 기술로는 보안이 여전히 도전과제이다. 그러므로 국내 보안 기업들은 여러 국내외의 벤더사의 하이브리드 클라우드 기술을 정확히 파악하고 해당기술을 활용하는 것이 중요하다. 이미 선진국의 보안 기업들은 하이브리드 클라우드 시장에서 패권을 장악하려는 추세이다. 우리나라의 보안 기업들도 클라우드 시스템 환경에 적합한 새로운 보안 기술을 신속히 개발할 것을 바라면서 적극적으로 연구에 매진해야 할 것이다.

참 고 문 헌

[1] http://korea.emc.com/corporate/glossary/hybrid-cloud.htm

[1] http://www.bloter.net/archives/211063

[2] http://www.noteforum.co.kr/news/index.htm?nm=26017

[3] http://www.windowsazure.com/ko-kr

[4] http://www.windowsazure.com/media/net/chappell_understanding01.png

[5] http://www.windowsazure.com/media/net/chappell_understanding02.png

[6] http://www.windowsazure.com/media/net/chappell_understanding03.png

[7] http://www.windowsazure.com/media/net/chappell_understanding04.png

[8] http://www.windowsazure.com/media/net/chappell_understanding05.png

[9] http://www.optenet.com/en-us/solutions-enterprise-hybrid.asp

[10] http://www.vmware.com/kr/cloud-computing/hybrid-cloud.html

[11] http://www.cloudstrategymag.com/ articles, "IBM Extends Bluemix With Cloud Service For The Internet Of Things Software As A Service", 2014. 10.17.

[12] https://openstacksummitmay2015vancouver.sched.org/event/c4a4143d2edec27045 affc527766ce07#.VVVgxbntlBc

[13] http://dcseurope.info/news_full.php?id=34300

[14] https://www-03.ibm.com/press/us/en/ pressrelease/44239.wss

[15] https://www.bloter.net/archives/219371

[16] 김학범, 전은정, 김성준, "클라우드 컴퓨팅 환경에서의 보안관리에 관한 연구", 경영컨설팅 리뷰 논문집, 제2권 제1호, 2011. 4.

[17] 정성재, 배유미, “클라우드 보안 위협요소와 기술 동향 분석”, 보안공학연구논문지, 제10권 제 2호 pp. 199~212, 2013년 4월
[18] 김태형, 김인혁, 민창우, 엄영익, “클라우드 컴퓨팅 보안 기술 동향”, 정보과학회지, 30(1), pp.30-38, 2012.
[19] https://www.fedramp.gov/about-us/about/
[20] FedRAMP-Control-Quick-Guide-Rev4-FINAL-01052015
[21] CONEX, "중국, 클라우드 시장 2020년 43억 달러 전망...정부 입김 강해 현지업체 주도 속 해외업체 부진", 2014년 7월 30일.
[22] [클라우드 보안] 한국판 '페드램프' 내년에 시행되나, 미디어잇, 2015.7.26.

〈저 자 소 개〉

박 준 현 (Jun-Hyun-Park)
2015년 3월~현재 : 동국대학교 국제정보대학원 정보보호학과 석사과정
관심분야 : 정보보호, 빅데이터분석 기술

박 재 승 (Jae-Seung-Park)
2015년 3월~현재 : 동국대학교 국제정보대학원 정보보호학과 석사과정
관심분야 : 정보보호

조 성 환 (Sung-Hwan-Cho)
2015년 3월~현재 : 동국대학교 국제정보대학원 정보보호학과 석사과정
관심분야 : 정보보호

전 환 웅 (Hwan-Ung-Jeon)
학생회원
2014년 2월 : 동국대학교 전산원 컴퓨터공학과 졸업
2015년 3월~현재 : 동국대학교 국제정보대학원 정보보호학과 석사과정
관심분야 : 정보보호, 사이버포렌식

전 은 정 (Eun-Jung JUN)
정회원
2006년 8월 : 순천향대학교 산업정보대학원 정보보호학과 졸업(공학석사)
2013년 2월 : 순천향대학교 일반대학원 정보보호학과 졸업(공학박사)
2012년 3월~현재 : (주)이지제이 대표이사
2015년 9월~현재 : 아주대학교 대학원 지식정보공학과 겸임교수
관심분야 : 개인정보보호

김 학 범 (Hak-Beom KIM)
정회원
1990년 8월 : 중앙대학교 대학원 전자계산학과 졸업(공학석사)
2001년 2월 : 아주대학교 대학원 컴퓨터공학과 졸업(공학박사)
1991년 10월~1996년 6월 : 한국전산원 주임연구원
1996년 7월~2001년 8월 : 한국정보보호진흥원 기술표준팀장
2001년 9월~2003년 1월 : (주)드림시큐리티 상무이사
2003년 2월~2005년 3월 : (주)장미디어인터렉티브 상무이사
2008년 4월~2009년 6월 : 인포섹(주) 수석컨설턴트
2009년 7월~2010년 12월 : 에스지에이(주) 연구소장
2001년 3월~2009년 2월 : 순천향대학교 정보보호학과 겸임교수
2005년 9월~현재 : 동국대학교 국제정보대학원 겸임교수
2011년 7월~현재 : 한국정보보호학회 이사
2015년 5월~현재 : 디지큐코리아(주) 부사장
관심분야 : ISO 27001, PIMS, ISMS, 클라우드컴퓨팅 보안, 개인정보보호