클라우드 서비스의 보안 취약점 및 위협

지도교수 : 김　　윤
연 구 자 : 박 태 준

< 목 차 >

요　약

서버, 스토리지, 데이터베이스, 네트워킹, 소프트웨어, 분석, 인텔리전스 등의 컴퓨팅 서비스를 제공함으로써 궁극적으로 모든 IT의 자원을 서비스화 하는 클라우드 컴퓨팅은 복수의 사용자가 언제, 어디서, 어떤 종류의 서비스를 얼마만큼 이용하더라도 장애 없이 편리하게 사용되고 있다. 반면 점점 보안 취약점이 속속 발견되고 있고 이에 따라 다양한 위협에 노출되어 있는 것도 사실이다. 이에 따라 데이터, 앱 및 인프라를 잠재적인 위협으로부터 보호할 수 있는 광범위한 정책 집합, 기술이 등장하고 있다.

주요어 :클라우드 서비스, 가상화, HDFS, 하둡, 스파크 엔진, 대규모 분산처리

1. 서론

1.1 클라우드 컴퓨팅

클라우드 컴퓨팅 이란 클라우드(인터넷)을 통해 가상화된 컴퓨터의 시스템 리소스(IT 리소스)를 요구하는 즉시 제공하는 기술을 뜻한다.

[사진 1] 클라우드 컴퓨팅 개념도

인터넷 기반 컴퓨팅의 일종으로 정보를 자신의 컴퓨터가 아닌 클라우드(인터넷)에 연결된 다른 컴퓨터로 처리하는 기술을 의미한다. [그림1]에 나오는 응용프로그램들을 어디서나 접근할 수 있는, 주문형 접근을 가능케 하는 모델이며 최소한의 관리 노력으로 빠르게 예비 및 릴리스를 가능케 한다.

클라우드 컴퓨팅과 스토리지 솔루션들은 사용자와 기업들에게 개인 소유나 타사 데이터 센터의 데이터를 저장, 가공하는 다양한 기능을 제공하며 도시를 거쳐 전 세계로까지 위치해 있을 수 있다.

클라우드 컴퓨팅은 전기망을 통한 전력망과 비슷한 일관성 및 규모의 경제를 달성하기 위해 자원의 공유에 의존한다. 지지자들은 클라우드 컴퓨팅을 통해 기업들이 선행 투자 인프라스트럭처 비용(예: 서버 구매)을 없앨 수 있다고 주장하고 있다.

그뿐 아니라, 단체들이 컴퓨터 인프라스트럭처에 시간과 비용을 들이는 대신 핵심 사업에 집중할 수 있게 하고 있다. 또, 클라우드 컴퓨팅을 통해 기업들이 자신들의 응용 프로그램의 기동 및 실행 속도를 더 빠르게 할 수 있게 하여 취급 용이성을 개선시키고 유지보수를 줄여줄 수 있게 도와주며 정보기술(IT) 팀들이 유동적이고 예측 불가능한 사업 수요를 충족시키기 위해 자원을 더 빠르게 조절할 수 있게 한다.

클라우드 제공자들은 일반적으로 종량제 모델을 사용하고 있다.

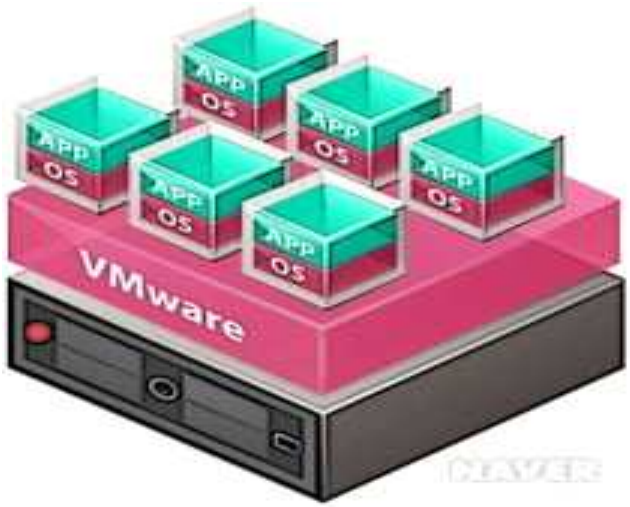
2.1 기술

클라우드 컴퓨팅을 구현하기 위해 필요한 기술에는 다음과 같은 것들이 있다.

- 가상화 기술 : 물리적인 하드웨어의 한계를 넘어서 시스템을 운용할 수 있는 기술

[그림2]를 보자. 가상화 기술에 대해 물리적으로 설명되어있다. 세부 설명=하드웨어, 저장장치 등의 물리적인 리소스의 특성들을 감추면서 IT 자원을 제공하는 기술

예를 들자면 서버 가상화를 통해 하나의 물리적인 컴퓨터 하드웨어에 동시에 1개 이상의 운영체제를 동시에 가동할 수 있다. 반대로 여러 대의 물리적 저장장치를 하나의 단일 논리 저장장치로도 이용할 수 있다.

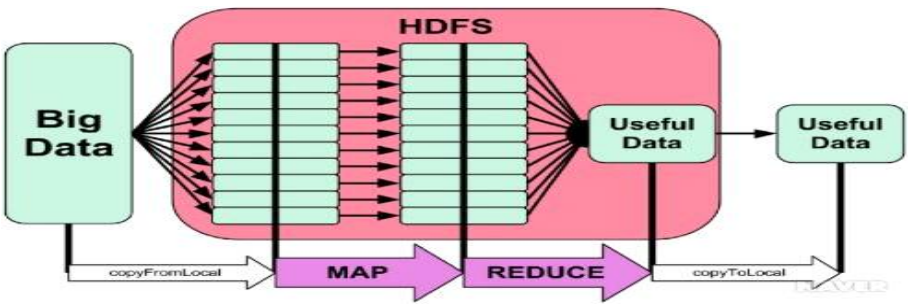


[사진 2] 가상화 개념도

- 대규모 분산처리: 대규모(수천 노드 이상)의 서버 환경에서 대용량 데이터를 분산 처리하는 기술인 하둡은 큰 컴퓨터 클러스터에서 동작하는 분산 응용 프로그램을 지원하는 프리웨어 자바 소프트웨어 프레임워크를 말한다.

복수의 컴퓨터를 논리적인 하나의 컴퓨팅 자원으로 이용할 수 있는 것으로 볼 수 있다. 핵심 구성요소는 여러 컴퓨터 노드에 대용량 파일을 나누고 중복시켜 안정성을 주는 분산 확장 파일 시스템인 HDFS와 분산 환경의 병렬데이터 처리기법인 맵리듀스 엔진을 말한다.

페이스북, 야후 등이 이를 사용하고 있다.



[사진 3] HDFS와 맵리듀스 개념도

- 오픈 인터페이스 : 인터넷을 통하여 서비스를 이용하고 서비스 간에 정보 공유를 할 수 있는 인터페이스 기술 클라우드 컴퓨팅 기반의 SaaS, PaaS 등에서 기존 서비스에 대한 확장 및 기능 변경 등에 적용한 API 기술은 전통적으로 한 ICT 자원의 서비스를 응용프로그램에서 이용하기 위해 발전해 왔다.
이는 웹 서비스의 활성화와 함께 누구나 이용하여 웹의 활용성 증대를 도모할 수 있도록 오픈 인터페이스로 확장되고 있다. 서비스의 활용성과 유용성의 증대를 위해서 외부에서 쉽게 기능을 활용할 수 있는 인터페이스 수요 충족에 이바지하고 있다.

- 서비스 프로 비저닝 : 서비스 제공자가 실시간으로 자원을 제공하는 기술, 서비스 신청부터 자원 제공까지의 업무를 자동화하여 클라우드 컴퓨팅의 경제성과 유연성 증가에 기여 세부 기술 자원 제공 동적 자원 프로 비저닝을 통한 확장성 및 탄력성을 제공한다.

- 자원 유틸리티 : 전산 자원에 대한 사용량을 수집하고, 이를 바탕으로 사용한 만큼만 비용을 지불하도록 하는 기술 개념이다.

- SLA(서비스 수준 관리) : 외부 컴퓨터 자원을 활용해서 클라우드 컴퓨팅 특성상 서비스 수준이라는 계량화된 형태의 운영 품질 관리가 필요하다.

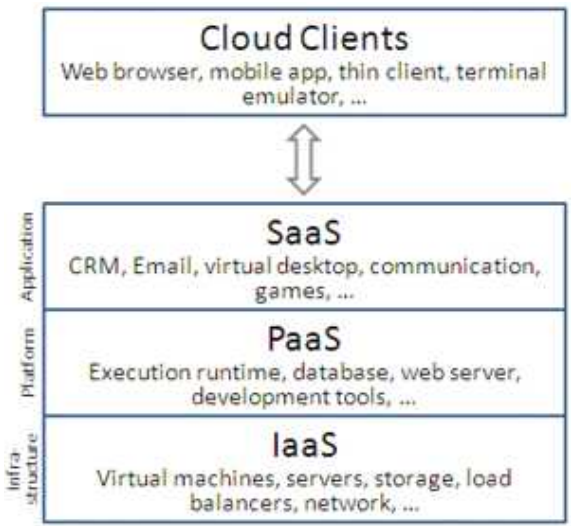
- 체제 보안 및 프라이버시 : 외부 컴퓨팅 자원에 기업 또는 개인의 민감한 정보를 저장함에 따라서 해당 정보에 대한 보안이 주요한 이슈로 부각되고 있다.

- 다중 공유 모델 : 정보자원 인스턴스를 여러 사용자 그룹이 완전히 분리된 형태로 사용하는 모델로서 서비스를 제공하는 데 필수 요소이다.

2. 본론

2.1 클라우드 컴퓨팅의 서비스 형태

SaaS(software as a Service)는 HW와 OS뿐만 아니라 응용 SW까지 제공하는 클라우드 서비스를 말한다. PaaS(Platform as a Service)는 운영체제와 SW 개발이나 데이터 분석을 위한 도구들까지 제공하는 클라우드 서비스이며 IaaS(Infrastructure as a Service)는 CPU, 메모리 등의 HW 자원을 제공하는 클라우드 서비스이다.



[사진 4] 계층별로 정렬된 클라우드 컴퓨팅 서비스 모델

2.2 장단점

장점으로는 비용과 지출이 적으며 휴대성이 높고 컴퓨터 가용률이 높은 편이다. 이러한 높은 가용률은 그린 IT 전략과 일치하며 다양한 기기를 단말기로 사용하는 것이 가능하고 서비스를 통한 일관성 있는 사용자 환경을 구현하는 것이 가능하다.

사용자의 데이터를 신뢰성 높은 서버에 보관함으로써 안전하게 보관 가능 컴퓨팅 자원을 유연하게 조절할 필요가 있는 영역에서 가장 효과적 고객이 특정 시점에 집중되는 영역은 클라우드 컴퓨팅이 매우 효과적 시스템 구축에 따른 리스크 조절 비용 관리 유용 필요할 때 필요한 만큼의 컴퓨팅 자원을 임대하는 클라우드 방식이 효과적 단기간에 대규모 컴퓨팅 자원이 필요한 인공지능 개발, 시뮬레이션 같은 분야도 클라우드 이용에 효과적이다.

단점은 유연한 컴퓨팅 자원 활용이 가능하지만, 최상의 안정성과 보안이 필요한 영역에서는 적용에 한계가 존재함 통상 클라우드 사업자가 제공하는 시스템 가용률은 99.95%로 온프래미스 환경에서 추구하는 99.999%에는 미치지 못하고 있다. 95%는 연간 4.4일, 월 21.6분의 장애 발생이 가능한 수준의 시스템 안전성을 의미한다. 24시간 365일 절대로 중단되어서는 안 되는 시스템인 경우, 클라우드 전환에 따른 리스크가 높다. 기업의 핵심 경쟁력과 관련된 공정 데이터 등의 처리는 인터넷과 연결되어 사용해야 하는 클라우드 환경과는 적합하지 않다.

3. 클라우드 컴퓨팅의 취약점 종류

- 데이터 유출

표적 공격의 주목표 사람의 실수나 애플리케이션 취약점 또한 잘못된 보안 관행의 결과일 수도 있다. 유출되는 데이터에는 개인 건강 정보, 금융 정보, 개인 식별 정보, 영업 비밀, 지적 재산을 포함한 온갖 종류의 정보가 포함된다. 조작의 클라우드 기반 데이터는 다양한 이유로 여러 사람들에게 가치가 있을 수 있다.
데이터 유출 위험은 클라우드 컴퓨팅에만 국한된 사항은 아니지만 클라우드 고객 입장에선 가장 큰 우려 사항이기도 하다.

- 불충분한 ID, 자격 증명 및 액세스 관리

합법적인 사용자, 운영자 혹은 개발자로 가장한 공격자는 데이터를 읽고 수정하고 삭제할 수 있다. 또한, 제어 및 관리 기능을 통해 전송 중인 데이터를 엿보거나 합법적인 소스를 가장해 만든 악의적인 소프트웨어를 배포할 수 있다. 결과적으로 ID, 자격 증명 또는 키 관리가 제대로 되지 않으면 데이터에 대한 무단 액세스를 허용하게 되고 조직이나 최종 사용자에게 치명적인 피해를 입힐 수 있다.

- 안전하지 않은 인터페이스와 API

클라우드 공급업체는 고객이 클라우드 서비스를 관리하고 상호작용하는데 사용하는 일련의 소프트웨어 UI(user Interfaces)나 API(Application Programming Interfaces)를 제공한다. 프로 비저닝, 관리, 모니터링은 모두 이런 인터페이스를 사용해 수행되며 일반적인 클라우드 서비스의 보안과 가용성은 API의 보안에 따라 좌우된다. 따라서 API는 정책을 우회하기 위한 우발적, 혹은 악의적인 시도를 차단하도록 설계되어야 한다.

- 시스템 취약점

시스템 취약점은 프로그램에 존재하는 악용할 수 있는 버그로, 공격자가 시스템에 침투해 데이터를 훔치고, 시스템 제어 권한을 탈취하거나 서비스 운영을 방해하게끔 해준다.
CSA는 “운영체제 구성요소 내에 있는 취약점이 있다면 모든 서비스와 데이터의 보안이 심각한 위험에 처하게 된다”라고 말했다. 클라우드에서 멀티 테넌시(multi-tenancy)가 확산되면서 다양한 조직의 시스템이 서로 밀접하게 위치하고 공유 메모리와 리소스에 액세스할 수 있게 되고 이는 새로운 공격 표면을 형성하게 한다.

- 계정 도용

계정 또는 서비스 도용은 새로운 것은 아니지만 클라우드 서비스로 인해 새로운 위협이 추가된 상황이다. 공격자가 사용자 자격 증명을 획득하게 되면 활동과 거래를 도청하고 데이터를 조작하고 위조된 정보를 반환하고 클라이언트를 불법적인 사이트로 돌릴 수 있다. 계정 또는 서비스 인스턴스는 공격자에게 새로운 기반이 될 수 있다. 자격 증명을 도용한 공격자는 종종 클라우드 컴퓨팅 서비스의 주요 영역에 액세스해 해당 서비스의 기밀성, 무결성, 가용성을 훼손 할 수 있다.

- 악의적인 내부자

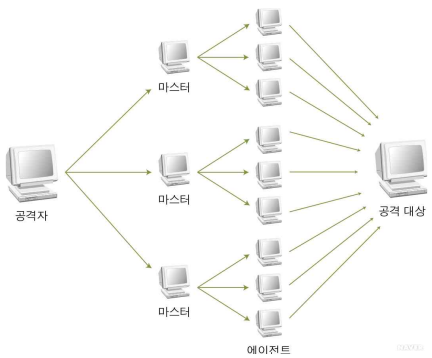
악의적인 내부자에 대한 위협의 수준은 논쟁의 여지가 있지만, 내부자 위협이 실체가 있는 적이라는 사실에는 논란의 여지가 없다. 시스템 관리자가 악의적인 내부자인 경우, 민감한 정보에 액세스할 수 있으며 매우 중요한 시스템과 데이터에 대한 더 높은 수준의 액세스 권한을 가질 수 있다. 클라우드 서비스 공급 업체에게 전적으로 보안을 맡기는 시스템은 더 큰 위험에 노출된다.

- APT

APT는 기생충 형태의 사이버 공격으로, 시스템에 침투해 목표 조직의 IT인프라 내에 활동 거점을 만들어 데이터를 훔친다. APT는 장기간에 걸쳐 은밀하게 목표를 공격하며 APT를 차단하는 보안 조치에 따라 자체적으로 적응하는 경우가 많다. CSA는 “일단 내부에 침입한 APT는 데이터센터 네트워크에서 횡으로 이동하며 정상적인 네트워크 트래픽 사이에 섞여 목표를 달성 한다”고 말했다.

- DOS

DoS(Denial of Service) 공격은 서비스 사용자가 데이터 또는 애플리케이션에 액세스할 수 없도록 한다. 공격자는 공격 대상 클라우드 서비스가 프로세서, 메모리, 디스크 공간, 또는 네트워크 대역폭과 같은 한정된 시스템 리소스를 과도하게 소비하도록 해 시스템 속도를 저하시키고 합법적인 서비스 사용자가 서비스에 액세스할 수 없도록 만든다. [그림3]을 보면 DOS 공격을 통한 네트워크 대역폭 리소스를 어떤 식으로 소비하도록 하는지 설명되어있다.



[사진 5] 분산 서비스 거부 공격도

- 스펙트라와 멜트다운

악의적인 자바스크립트 코드를 사용해서 암호화된 데이터를 비롯한 콘텐츠를 메모리에서 읽을 수 있게 해주는 대부분의 최신 마이크로프로세서의 설계 오류를 공개했다.

멜트다운(Meltdown)과 스팩트라(Spectre)는 스마트폰에서 서버에 이르기까지 모든 장치에 영향을 미친다. 특히 스펙트라의 위협 특성으로 인해 클라우드 위협 목록에 추가됐다.

스펙트라와 멜트다운은 애플리케이션 사이에 차단을 없애기 때문에 부채널 공격을 허용한다. 권한이 없는 로그인을 통해 시스템에 액세스할 수 있는 공격자는 커널에서 정보를 읽거나 공격자가 게스트 가상 머신의 관리자일 경우, 호스트 커널을 읽을 수 있다. 이는 클라우드 서비스 제공 업체에게는 큰 문제로 제기된다.

패치가 이뤄지면 공격을 실행하기 어려워진다. 다만 이 패치로 인해 성능이 저하될 수 있으므로 일부 기업에서는 시스템들을 패치를 적용하지 않은 상태로 둘 수 있다. CERT는 영향을 받은

모든 프로세스를 대체할 것을 권장하고 있다. 아직까진 멜트다운이나 스펙트라를 활용한 알려진 악용 사례는 존재하지 않는다.
하지만 전문가들은 가능성이 상대적으로 높다는 것에 동의한다. 클라우드 공급업체가 이를 방지하는 가장 좋은 방법은 최신 패치가 있는지 확인하는 것이다.
기업 고객은 클라우드 공급업체가 멜트다운과 스펙트라에 대해 어떻게 대응하고 있는지 정보를 요구해야 한다고 생각한다.

- 데이터 손실
CSA는 “클라우드 내 저장된 데이터는 악의적인 공격 이외 다른 이유로 손실될 수 있다”고 말했다. 클라우드 서비스 공급업체가 실수로 삭제하거나 화재나 지진과 같은 물리적인 재해를 당할 경우, 클라우드 공급업체나 소비자가 데이터 백업, 재해복구 등의 비즈니스 연속성에 대한 모범 사례에 따라 적절한 조치를 취하지 않았다면 데이터를 영구적으로 손실할 수 있다.

- 불충분한 실사
경영진은 비즈니스 전략을 수립할 때, 클라우드 기술과 서비스 공급업체를 고려해야 한다고 CSA는 말했다. 공급업체를 평가할 때 실사를 위한 효과적인 로드맵과 체크 리스트를 만드는 것이 필수적이다. 클라우드 기술을 급하게 도입하고 실사 없이 공급업체를 선택하는 조직은 여러 가지 위험에 노출된다.

- 클라우드 서비스 남용과 악의적인 사용
보안이 취약한 클라우드 서비스, 무료 클라우드 서비스 평가판, 결제 수단 사기를 통한 사기성 계정 등록은 클라우드 컴퓨팅 모델을 악의적인 공격에 노출 시킨다. 공격자는 클라우드 컴퓨팅 리소스를 활용해 사용자, 조직 또는 다른 클라우드 공급업체를 공격 대상으로 삼을 수 있다. 클라우드 기반 리소스 악용의 사례에는 DDos 공격, 이메일 스팸 및 피싱 사기 등이 있다.

- 공유 기술 취약점
클라우드 서비스 공급업체는 인프라, 플랫폼 또는 애플리케이션을 공유함으로써 서비스 확장성을 제공한다. 클라우드 기술은 기존 하드웨어/소프트웨어를 대폭 변경하지 않고도 서비스 형태의 주문을 소화할 수 있는데, 종종 그 대가로 보안이 희생된다.
클라우드 서비스를 지원하는 인프라의 기반 구성요소가 멀티 테넌트 아키택처 또는 다중 고객 애플리케이션을 위한 강력한 격리 특성을 제공하도록 설계되지 않은 경우도 있다.
이로 인해 모든 제공 모델에서 악용될 가능성이 있는 공유 기술 취약점이 발생할 수도 있다.

4. 문제해결방안

4.1기술 내적 보안책

- 보안 전략

공유 자원의 사용으로 새롭게 야기되는 위협에 대해 기존의 보안 방식의 재구성을 통한 방어 체계를 구축한다.

- 전송 데이터의 보호

인터넷으로 사용자의 데이터를 클라우드 서버에 전송할 때 발생할 수 있는 보안 문제에 대해 TLS, SSH, VPN을 혼합 사용함으로써 해결이 가능하다.

- 데이터의 저장

① 클라우드 스토리지는 사용자의 데이터가 저장되는 시스템으로 저장 데이터에 대한 암호화를 활용한다.
② 클라우드의 서비스 별로 저장되는 데이터는 상이하며, 데이터의 민감도와 공유 여부, 규제 대상 여부를 고려하여 암호화 및 격실 조치를 수행한다.
③ 암호화는 사용자 개별단위로 이루어지며, 최소한 AES-256과 같은 산업 표준 대칭 암호화 알고리즘을 활용하는 방식으로 보안성을 확보한다.
④ 데이터의 유실을 방지하기 위한 방법으로 DLP 정책의 일환으로 네트워크 단에서 외부 트래픽을 모니터링하고 차단하는 방식을 활용한다.

- 접근 및 인증

① FLdM을 활용한 사용자의 ID 인증을 통해 클라우드 접속 사용자를 인증하는 행위이다.
② 현재의 휴대폰 인증번호 입력과 유사한 개념으로 클라우드 상에서 ID관리의 어려움을 효과적으로 줄여준다.
③ 또한, 보안 사고에 대비하여 로그 데이터를 분리된 SIEM에 전송함으로써 효과적인 대응을 모색할 수 있다.

- VM간 독립성

① 사용자가 접근하는 VM간의 완벽한 독립성을 제공하여 클라우드 환경 내에서 다른 VM의 데이터와 트래픽을 도청하지 못하게 한다.
② 데이터는 암호화된 형태로 저장하고, 추후 삭제하더라도 저장소 어딘가에 남아있을 데이터에 대한 열람은 불가하도록 조치한다.
③ 네트워크 트래픽에 대해서는 약간의 성능 저하를 감수하더라도 앞서 언급한 TLS, SSH, VPN을 통합 활용한다.

- 침입 탐지 : 가상머신 내부정보 분석 기반 침입 탐지

- 하이퍼 바이저 방식 탐지
① 하이퍼바이저를 통해서 각 가상머신의 내부 상태를 분석하고 침입을 탐지하는 기법
② 가상머신의 vCPU의 내용, 파일IO활동, 각 VM들이 발생시키는 네트워크 패킷 캡쳐 같은 내부 정보에 대한 분석을 통해 악성 행위를 탐지한다.
③ 하이퍼 바이저상에서IPS 기능 및 방화벽, 안티바이러스 등의 서비스를 제공한다.

- VM 방식 탐지
에이전트리스 가상 보안 탐지기법으로 각 가상머신 내에서 에이전트 방식으로 동작하지 않고 별도의 특별한 권한을 가진 보안 전용의 가상머신 상에서 동작한다.

- 어플리케이션 보안
클라우드와 같은 공유 환경에서 동작하는 응용 프로그램에 대해서는 설계 시 종합적인 위협요소를 고려하여 설계한다.

4.2 기술외적인 보안책

- 보안 인증 체계
① 클라우드 보안 인증체계를 통한 보안 표준을 준수한다.
② ITU-T와 ISO/IEC JTC 1을 중심으로 한 국제 공적 표준기구에서 클라우드 보안인증 서비스를 제공한다.

- 보상 및 보험
① 클라우드 보안 사고 발생 시, 보상하는 제도 및 보험을 통한 사고대응 방안이 존재한다.
② 클라우드 SLA를 통해 데이터보호, 계정관리, 어플리케이션 운용 등 서비스 레벨 관리에 대한 약정을 진행한다.

-지리적 분산
지리적으로 분산된 데이터센터의 화재, 단전, 등의 비상사태 발생 시 빠른 대응을 위한 안전 시스템 및 데이터 센터 내의 출입관리와 침입방지 등의 철저한 보안관리 측면에서 안정성을 보장한다.

- 스펙트라, 멜트다운 완화 조치

- 하드웨어 OEM의 CPU 마이크로 코드/펌웨어와 함께 공급 업체의 소프트웨어 데이터를 적용하는 것 외에 현재 알려진 완화 조치가 알려지지 않았으며 운영체제를 통해서만 적용이 가능하다.

5. 결론

클라우드 컴퓨팅 환경이 전통적인 IT 환경을 대체하면서 가장 큰 화두로 등장한 것이 클라우드 보안이다. 클라우드 컴퓨팅은 기존 IT 기술의 연장선상에 있는 기술로서 보안상의 문제나 위협들도 대부분 기존의 보안 기술로 적용이 가능하다.

그러나, 일반적인 컴퓨팅 환경과 클라우드 컴퓨팅 환경의 가장 큰 차이점은 하이퍼 바이저를 이용한 가상화 환경이라고 볼 수 있다. 현재 가상화 기반 환경에 대한 다양한 취약점을 노출하고 있고, 관련 보안 제품들이 거의 없는 실정이다.

클라우드 컴퓨팅 환경이 안정적인 IT 환경의 기반 역할을 수행하기 위해서는 하이퍼 바이저 기반 보안 기술에 대한 연구가 더욱 필요할 것으로 여겨진다.

참고문헌

[1]클라우드 컴퓨팅 위키백과 https://ko.wikipedia.org/wiki
[2]클라우드 컴퓨팅 기술https://terms.naver.com/entry.nhn
[3]지형 공간정보체계 용어사전 DDOS 분산 서비스 거부[Distributed Denial of Service] https://terms.naver.com/
[4]클라우드 보안의 핵심이슈와 대응책-https://spri.kr/download/21793