Issue Report

2017. 12. 11. 제2017-006호

클라우드 보안의 핵심이슈와 대응책

Key Issues and Countermeasures in Cloud Security

안성원 (swahn@spri.kr)†
유호석 (hsy@spri.kr)
김다혜 (sdf3265@naver.com)

SPRi 소프트웨어정책연구소

○ 이 보고서는 「과학기술정보통신부 정보통신진흥기금」을 지원받아 제작한 것으로 과학기술정보통신부의 공식의견과 다를 수 있습니다.

○ 이 보고서의 내용은 연구진의 개인 견해이며, 본 보고서와 관련한 의문사항 또는 수정・보완할 필요가 있는 경우에는 아래 연락처로 연락해 주시기 바랍니다.

- 소프트웨어정책연구소 안성원(swahn@spri.kr) 선임연구원

《 요 약 문 》

클라우드 컴퓨팅은 세계적으로 활용률이 높아지고 있으나 국내에서는 도입과 확산이 저조한 편으로, 그 큰 원인 중 하나는 보안에 대한 우려 때문인 것으로 조사되었다. 그러나 클라우드 컴퓨팅의 보안은 일반적인 정보 보안과 본질적으로 다르지 않으며, 공유자원의 사용으로 새롭게 야기되는 위협에 대해서도 기존 보안기술을 재구성한 방어체계를 통해 현재의 정보 보안 수준으로 해결이 가능하다. 이 보고서에서는 기존 클라우드 컴퓨팅의 보안 위협에 대한 관점을 종합하고, 기술 및 기술외적인 측면에서 다양한 해결방안을 살펴보면서, 클라우드 컴퓨팅 보안에 대한 인식전환이 필요함을 설명하고 있다.

《 Executive Summary 》

Cloud computing is growing globally, but the adoption and diffusion of cloud computing is slow in Korea. One of the major causes was the concern of security. However, the security of cloud computing is not fundamentally different from general information security, and new security threats caused by the use of shared resources can be solved by the existing information security level through a defense systems that reconstruct existing security technology. This report summarizes the viewpoints of security threats of existing cloud computing, explores various solutions in terms of technology and non-technology, and explains the necessity of changing awareness of cloud computing security.

《 목 차 》

《 Contents 》

1. 연구배경

□ 클라우드 보안우려에 대한 재검토 필요

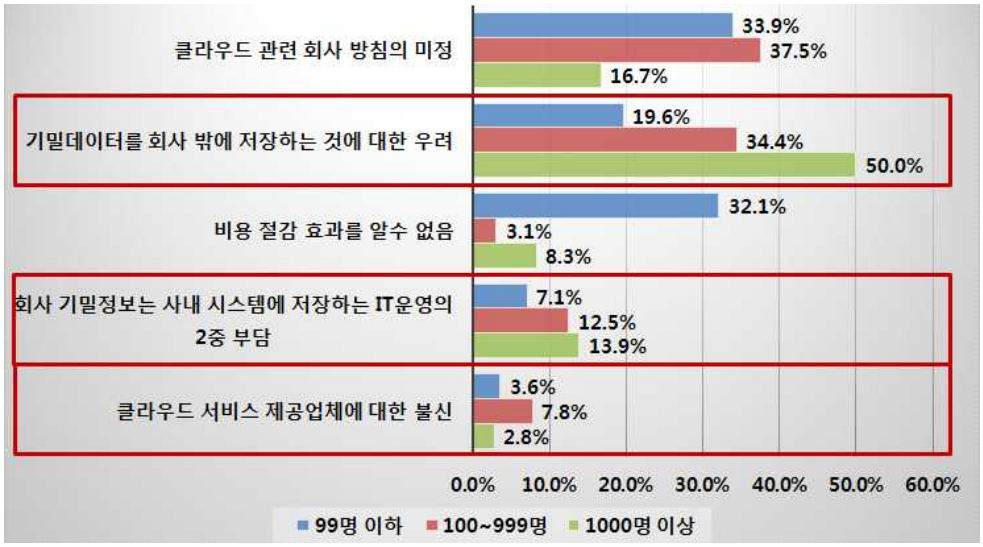
○ **(낮은 클라우드 도입율)** 선진국에서는 클라우드 도입이 활발*하나 국내는 전체기업 중 4.1%, 중소기업 중 8.8%** 만이 클라우드를 도입하여 OECD 35개 국 중 27위 수준으로 최하위권임

* 미국기업은 40% 이상(`12년), 일본기업은 33.1%(`13년)가 클라우드 도입·이용

* 한국정보화진흥원(2016), 통계청(2016)

○ **(도입율 저하 원인)** 국내 클라우드 컴퓨팅 활용률이 떨어지는 이유 중 하나는 기밀데이터의 유출, 클라우드 사업자에 대한 불신 등 **보안상 우려** 때문

* 응답기업의 33%와 1천명 이상 규모의 기업 50%가 보안을 클라우드 도입의 장벽으로 제기(2016, IDC)하였으며, 그 외 서비스 제공업체에 대한 불신, 기밀정보의 별도 운영 등 기타 보안관련 우려도 다수 존재



※ 출처 : 안랩, 클라우드 보안 위협 및 대응 방안, AWS summit, 2016 (재편집)

[그림 1-1] 클라우드를 도입하지 않는 이유

○ **클라우드 보안에 대한 정확한 분석 필요**

- 기존 클라우드 보안에 관한 논의들은 일반보안과 클라우드 보안이 혼재

- 클라우드가 기존방식 보다 보안에 더 취약한 것인지에 대한 정확한 정보를 제공하여, 클라우드 보안에 대한 부정적인 인식을 개선할 필요

2. 클라우드 컴퓨팅의 개요와 이슈

2.1. 클라우드 컴퓨팅의 개요

□ **(개념)** 클라우드 컴퓨팅(Cloud Computing)은 필요시에 편리하게 컴퓨팅 자원에 접근하여 데이터를 처리하고 연산을 수행할 수 있도록 네트워크, 서버, 스토리지, 애플리케이션을 연결해 놓은 컴퓨팅 제공 방식

○ **(유래)** 2006년 구글직원이 유휴 컴퓨팅 자원의 재활용을 제안하면서 용어를 사용한 이후, 같은 해에 아마존이 AWS(Amazon Web Service)를 개시하며 사업을 시작

○ **(분류)** 클라우드 컴퓨팅은 서비스 모델에 따라 SaaS·PaaS·IaaS로, 배치방식에 따라 Public·Private·Hybrid로 구분 ([부록 1] 참조)

□ **(장점)** 서비스 제공자는 효율적으로 컴퓨팅 자원(Computing Resource)을 재사용할 수 있고, 서비스 이용자는 필요한 시점에 필요한 만큼만 컴퓨팅 자원을 빌려서 쓸 수 있음

○ **(효율성)** 컴퓨팅자원 구매과 유지보수에 들어가는 비용이 절감되고, 사전에 환경을 구축하기 위한 공간확보와 인력채용과 같은 고정비용이 없음

○ **(민첩성)** 컴퓨팅 자원을 조달하는 시간을 획기적으로 단축하여 사업을 개시할 수 있고, 용량증설이 필요할 경우 자원을 요청하여 즉시 확장이 가능

□ **(확산)** 사물인터넷(IoT), 빅데이터 등의 도입으로 클라우드 컴퓨팅을 통한 데이터 트래픽이 전체의 76%를 차지할 정도로 확산이 가속화 ([부록 2] 참조)

※출처 : K-ICT 클라우드컴퓨팅 활성화 계획, 2015.

[그림 2-1] 글로벌 ICT 패러다임의 변화

2.2. 클라우드 컴퓨팅 보안의 핵심이슈 : ‘공유자원’ 문제

□ **(보안에 대한 우려)** 클라우드의 특성상 **저장된 데이터의 정확한 위치를 가늠하기 어렵고, 산재**되어 있다는 점이 보안 우려의 주요인

○ 특히, Public 클라우드를 사용했을 때 외부 공간에 민감한 **데이터를 클라우드 상에 저장하는 것에 대한 신뢰성과 안정성에 의문**을 제기

* 민간 기업 45.2%, 공공기관 35.0%가 클라우드 도입 시 데이터 보호를 가장 중요하다고 응답(클라우드산업실태조사(NIPA), 2015)

○ 클라우드 및 보안 관련한 각 기관과 학회 등은 클라우드 서비스의 보안 위협요소에 대하여 다양하게 정의하고 있음 ([부록 3] 참조)

* CSA(Cloud Security Alliance)[1]에서는 가장 최신의 분류 기준으로 보안 위협 요소를 12가지로 정의 하며, NIST(미 표준기술연구소), Gartner, UC Berkeley등도 각각 클라우드의 위협 요소를 각각 8, 7, 10 가지 요소로 나누어 정의

□ **(보안문제의 재분류)** 클라우드 등장 이전(전산실과 데이터센터)부터 **이미 존재하던 보안위협**과 클라우드가 야기하는 새로운 보안위협인 **‘공유자원’** 문제를 분리하여 접근할 필요가 있음

○ 특히, Public 클라우드에서 기업 간 컴퓨팅자원을 공유하면서 생긴 새로운 보안우려에 집중한 대책 검토가 필요

<표 2-1> 클라우드와 기존 시스템의 자원공유 범위

분류	설명	자원공유 범위
Public 클라우드	▪ 기업이 소유한 컴퓨팅 자원 없이 서비스 업체가 보유 및 제공하는 자원을 나누어 사용하고 사용량에 따라 과금	기업 간에 컴퓨팅 자원을 상호 공유
Private 클라우드	▪ 데이터센터에 가상화 기술을 적용하되, 기업별로 소유한 컴퓨팅 자원을 기업 내에서 공유	기업마다 전용 컴퓨팅 자원을 보유
데이터센터	▪ 기업 내부 전산실의 컴퓨팅 자원을 기업 외부의 데이터 센터에 위탁	
전산실	▪ 클라이언트-서버 환경에서 서버와 스토리지를 담당 부서에 일임하고 집중배치	

1) 클라우드 컴퓨팅의 안정성 증진 및 사용자 교육을 목적으로 만든 비영리 기관으로, 보안실무자 컨퍼런스인 ISSA Forum의 2008년 개최 모임에서 탄생

* (공유자원 문제) 서버OS를 공유하기 위해 가상영역으로 분리해 주는 '가상화 기술'과 응용SW를 여러 기업이 공유 사용하게 해주는 'Multi-Tenancy'는 클라우드를 가능하게 하는 핵심기술이나 이로 인해 보안의 경계가 겹치는 문제가 발생할 수 있음

<표 2-2> 클라우드 보안 위협과 구분

범주구분	위협의 예	위협 구분
가상화 문제	▪ VM탈출・호핑・이미지 변조, 하이퍼바이저 기반 루트킷	클라우드의 공유자원 문제
중복된 신뢰경계	▪ Multi-Tenancy로 인한 보안경계의 중첩	
네트워크 침입	▪ 네트워크 트래픽 도청, 악의적인 중간자	기존의 보안 문제와 동일
서비스 공격	▪ 서비스왜곡, 래핑, 웹서비스언어 스캐닝	
권한 탈취	▪ 접근 권한의 위·변조,식별자 관리・익명화	
과부하 공격	▪ DoS, DDoS 공격, 가상머신의 급격한 생성	
구현오류	▪ 설계 결함 등을 취약점으로 악용	

※자료: 클라우드컴퓨팅-개념,기술,구축체험 ,홍릉출판사, 2016 (재편집)

○ 그러나, Public 클라우드 업체의 보안사고 중 대부분은 일반적인 데이터센터에서도 동일하게 발생하는 사고유형이며, 일부 사례만이 Public 클라우드 상의 공유자원 문제로 분석됨

<표 2-3> 클라우드 보안사고 사례로 살펴본 위협의 범주

클라우드 업체	보안사고사례	범주
MS	2010년 서비스 환경설정 오류로 인해 클라우드상의 기업 정보가 타인에게 열람됨	중복된 신뢰경계 (공유자원)
아마존	2011년 아마존의 가상서버를 임대하고 가명으로 가입 후 가상서버를 좀비PC화하여 소니플레이스테이션 네트워크 해킹	가상화문제 (공유자원)
	폭풍우로 인한 정전사고로 EC2 장애, 협력서비스 업체인 넷플릭스, 핀테스트, 인스타그램 등 서비스 중단	자연재해
구글	2010년 태국의 ISP를 이용한 세션하이재킹 공격 발생	네트워크 침입
	2011년2월, 50만명의 이용자가 메시지 및 주소록이 사라지는 사고 발생	구현오류
	일본 대지진으로 인한 해저케이블 손상으로 Gmail, 안드로이드 마켓 접속 지연	자연재해
애플	2014년,유명 여배우들의 계정탈취를 통한 누드사진 유출	권한 탈취
	2012년,iCloud,Gmail, Twitter계정분석을 통한 맷호난 기자의 계정탈취 및 모든 개인자료 삭제	권한 탈취
	2011년, 모바일 마이그레이션에 따른 서버 과부화로인한 icloud 접속 불가	구현오류
VMWare	2012년,VmwareImage에 CRISIS 악성코드 삽입	악성코드
Dropbox	2012년,이용자 이메일 명단 유출 및 스팸 전송	직원계정 해킹

에버노트	2013년2월,백도어 활동, C&C 서버의 수집정보 은닉장소로 에버노트 이용	악성코드
Vaserv .com	2009년6월,가상화 플랫폼(Hyper-VM)에 대한 제로데이 공격으로 10만 고객사 웹사이트 삭제	SW취약점 해킹
Zen Desk	2013년2월,Adobe의 ZenDesk 시스템 해킹을 통한 협력회사(트위터, 핀터레스트, 텀블러) 개인정보유출	SW취약점 해킹
Dream Host	2012년1월,DreamHostDB해킹으로 인한 개인정보유출	SW취약점 해킹
KT	2012년 유클라우드(uCloud) 서버 스위치와 스토리지 오작동으로 인한 서비스 장애 발생	시스템오류
코드 스페이스	DDoS공격으로 모든 자원 삭제	과부하 공격
후지쯔	2011년, 후지쯔 클라우드 서비스 Dos공격으로 장애 발생	과부하 공격
세일즈 포스	2012년, 스토리지 저장 실패로 인한 서비스 중단	구현오류
First Server	시스템 업그레이드 중 오류 발생하여 5,693개 회사의 데이터 손실	관리문제

※ 자료 : 한국클라우드보안협회,CSA Summit Korea 2013., 삼정KPMG경제연구원,Issue Monitor 2016, 금융보안원,클라우드 컴퓨팅 개념과 산업동향,2016., 언론 기사 편집

○ 이 보고서에서는 클라우드의 '공유자원' 기술을 세부적으로 분석하고 위협요소 및 보안책을 살펴보고자 함

* 보안위협에 대한 분류는 전통적으로 기술적, 관리적, 물리적 측면의 위협으로 정의하나, 이 보고서에서는 기존의 보안 문제를 상속 받는 경우와 공유자원 환경을 통해 새롭게 야기되는 문제로 분류하고, 이를 기술적·기술외적인 측면으로 살펴보고자 함

* 다양한 클라우드 보안 위협에 대해 재정리 하면 다음과 같음

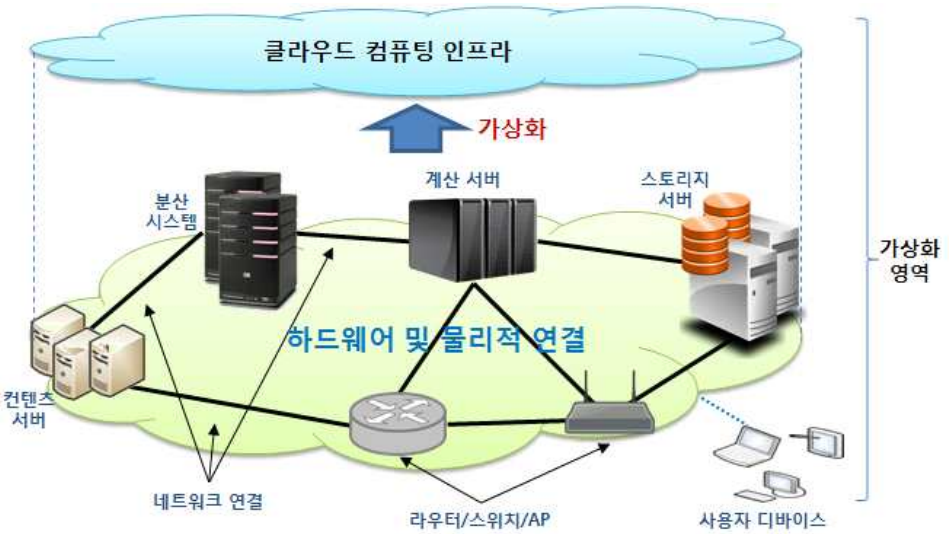
<표 2-4> 클라우드 보안 위협에 대한 재정리

구분	위협요소	세부항목 및 내용	CSA 분류 매핑
기술적	기존 보안 위협	▪ 네트워크 트래픽의 도청 및 위변조 ▪ 인증 및 접근권한 탈취에 따른 데이터 유출·손실 ▪ 서비스 거부(DoS, DDoS) 공격 ▪ 시스템 설계상의 오류	데이터유출, 불충분한 신분(접근)관리, 불안전한API, 시스템 취약점, 계정탈취, DDoS공격, APT공격
	가상화를 통한 위협	▪ 하이퍼바이저 감염 ▪ VM내부공격 및 이로 인한 침입탐지 어려움 ▪ 가상머신의 이동성에 따른 보안 문제	공유기술 취약점, 데이터유출, 시스템 취약점, APT공격
기술외적	관리측면 문제	▪ 내부자의 설계/관리 실수 ▪ 사용자의 계정정보 유출 ▪ 다양한 해커들에게 해킹의 빌미를 제공 ▪ 피해규모의 확산 ▪ 데이터센터 건물 관리 ▪ 화재, 지진 등의 재해로 인한 데이터 센터의 물리적인 피해와 이로 인한 데이터 유실	악의적 내부자, 데이터 유실, 불충분한 실사, 불손한 사용, 공유기술 취약점
	법제도 문제	▪ 지리적으로 분산된 인프라의 경우 국가별 상이한 법체계로 달라지는 정책과 자원 통제력 문제	불충분한 실사

3. 클라우드 컴퓨팅의 ‘공유자원’ 기술

3.1. 클라우드 기술의 개관

□ 클라우드 컴퓨팅 환경을 구현하기 위해서는 가상화, 분산처리, 네트워크에 관련한 컴퓨팅 자원이 필요하며 이들을 네트워크로 연결하여 통합된 계산, 저장 및 처리를 수행



[그림 3-1] 클라우드 컴퓨팅을 위한 하드웨어 연결과 가상화의 예

○ **가상화(Virtualization)**는 물리적인 컴퓨터 자원을 추상화 하는 것을 의미하는데, 마치 하나의 장비를 여러 개처럼 동작시키거나 반대로 여러 개의 장비를 묶어 사용자에게 공유자원으로 제공하는 클라우드의 핵심기술

- 하드웨어 장비를 가상화하면 해당 장비가 제공하는 자원(Resource)의 활용도를 높여 비용절감의 효과가 있음

* 가상화 자원은 크게 CPU, 메모리(Memory), 스토리지(Storage), 네트워크 (Network) 가상화로 분류
* CPU 가상화 : 각각의 가상머신(VM)에 동적인 CPU 할당
* 메모리 가상화 : VM에 메모리 영역을 할당하며, 연속된 물리적 메모리가 존재하는 것처럼 인식
* 스토리지 가상화 : VM에 저장소를 할당하며, 직접 연결된 디스크처럼 인식
* 네트워크 가상화 : VM에 물리적인 네트워크 인터페이스(NIC)를 공유하여, 가상의 NIC을 할당

- 가상네트워크(VLAN)은 물리적 네트워크에서 분리된 가상의 네트워크를 제공함으로써 네트워크의 유동적인 관리와 성능조율이 가능

  * 예) 특정 서비스를 제공하는 가상네트워크를 구성하여, 사용자, 서비스 목적, 과금 체계별로 독립된 네트워크를 제공

- 스토리지영역 네트워크(SAN)는 물리적 저장 디바이스를 가상화하며 스토리지 리소스의 가용성과 유연성을 향상

  * 예) 특정 서버나 저장소에 데이터의 저장 요구가 많아지는 경우 상대적으로 저장 공간이 남아 있는 저장소에 분산 저장

가상화와 하이퍼바이저

- 장비에 장착되어 있는 하드웨어를 가상화하기 위해서는 하드웨어들을 관장할 가상머신모니터(VMM: Virtual Machine Monitor)와 같은 중간관리자가 필요

  - 이 중간관리자를 하이퍼바이저(Hyperviser)라고 하며, [그림 3-2]와 같은 시스템 개념도상 하이퍼바이저의 위치 및 역할 차이에 따라 Type1과 Type2로 구분

※주) VM : Virtual Machine(가상머신)
※이미지 출처 : 안성원, 클라우드 컴퓨팅과 인공지능의 만남, IT데일리 전문가 강좌, 2017.7

[그림 3-2] 가상화의 종류

※ Type1은 일반적으로 하이퍼바이저(Hyperviser)형 가상화라고 하며, 하드웨어상에 가상머신을 관리하기 위한 VMM을 직접 동작시키는 방식으로, 하드웨어를 관장하기 위한 호스트 운영체제(OS)가 필요 없는 형태

※ Type2는 일반적으로 호스트(Host)형 가상화라고 하는데, 하드웨어상에 호스트 운영체제가 설치되어 있고, 이 호스트 운영체제 상에 설치되어 하이퍼바이저 역할을 수행하는 VMM이 가상머신을 동작시키는 방식

○ **분산처리(Distributed Computing)**는 클라우드를 위한 요소기술로 여러 대의 컴퓨터 계산 및 저장능력을 이용하여 커다란 계산문제나 대용량의 데이터 저장을 해결하는 방식

- 광의적으로는 여러 개의 컴퓨팅 디바이스를 하나의 시스템 안에 결합시킨 병렬컴퓨팅을 포함

  * 예) 그리드컴퓨팅(Grid Computing)은 많은 계산량을 필요로 하는 작업을 위해, 인터넷상으로 분산된 자원을 공유하여 가상의 슈퍼컴퓨터처럼 활용

○ **네트워크(Network)**는 물리적으로 떨어져 있는 다양한 장비들을 연결하기 위한 수단으로 중계장치(라우터, 스위치 등)의 가상화를 통해 가상네트워크(Virtual Network)를 지원

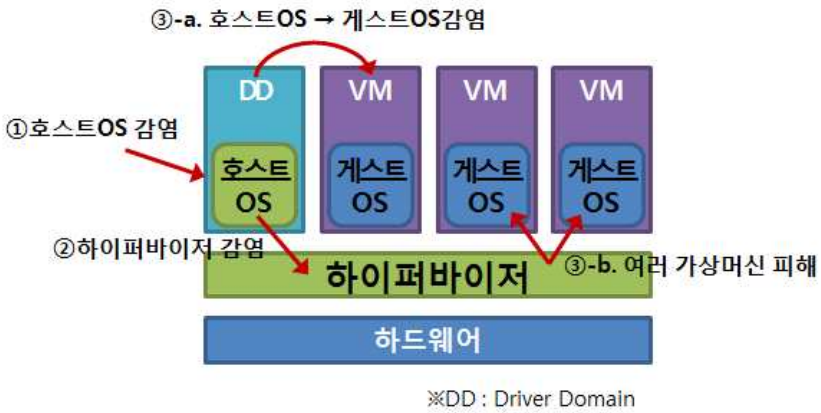
- 다양한 장비들을 네트워크로 연결하여 하나의 군집(Cluster)을 만들고 리소스를 활용

  * 예) 네트워크컴퓨팅(Network Computing)은 응용프로그램을 서버(Server) 상에 두되 작동은 사용자(Client)의 자원을 이용하는 방식

3.2. 기술적 측면의 위협

□ **(가상화로 인한 보안 문제)** 가상화 환경으로 인해 발생할 수 있는 보안 문제로 기존 보안 문제가 가상화로 인해 방어가 어려워지거나 파급효과가 커지는 문제

○ **(하이퍼바이저 감염 위험)** 클라우드 서비스를 구동하기 위해 필수적인 가상화 시스템 내 하이퍼바이저가 취약할 경우 이를 활용하는 여러 개의 가상머신(VM)이 동시에 피해를 입을 가능성

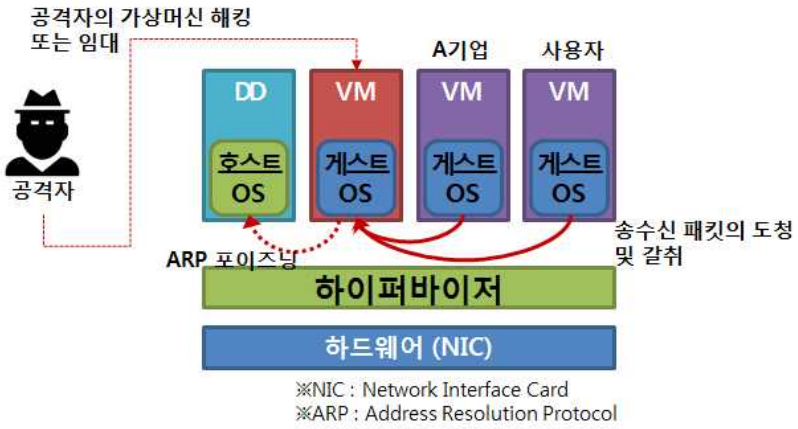


[그림 3-3] 가상머신 간 해킹

* 하이퍼바이저의 보안성이 낮다면 권한 탈취로 인해 해당 서버에서 구동되는 모든 VM 사용자들에게 피해를 줄수 있음

* 호스트OS의 감염을 통해 하이퍼바이저 및 타 VM내의 게스트OS로 감염 확산이 가능

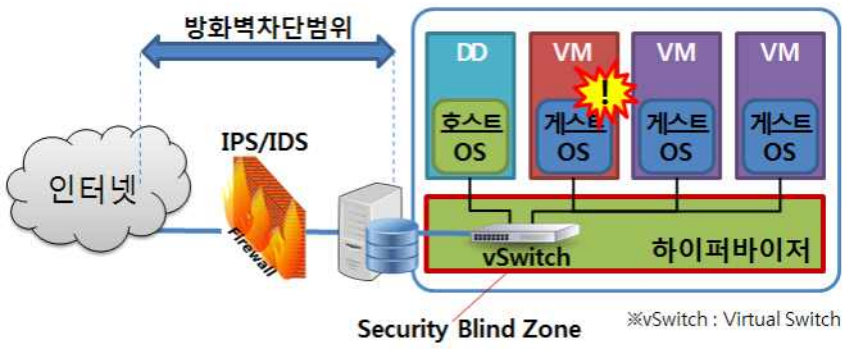
○ **(가상머신 공격 경로)** 사용자의 가상머신들이 상호 연결되어 내부의 가상머신에서 다른 가상머신으로의 패킷스니핑, 해킹, DDoS 공격, 악성코드 전파 등의 공격경로가 존재



[그림 3-4] 가상 네트워크를 통한 패킷 스니핑

○ **(공격자의 익명성)** 가상환경에서는 공격자가 누군지를 파악하기가 어려워 기존 네트워크 보안기술(방화벽, IPS[2]/IDS[3])로는 가상화 내부 영역에 대한 침입탐지가 어려움

* 예) 아마존웹서비스(AWS)를 통한 웹호스팅 시 보안 문제가 발생했을 때, 여기에 접속한 이들이 어떤 서비스를 어떻게 구동하는지 알기 어렵기 때문에 누가 공격을 수행했는지 알기 어려움



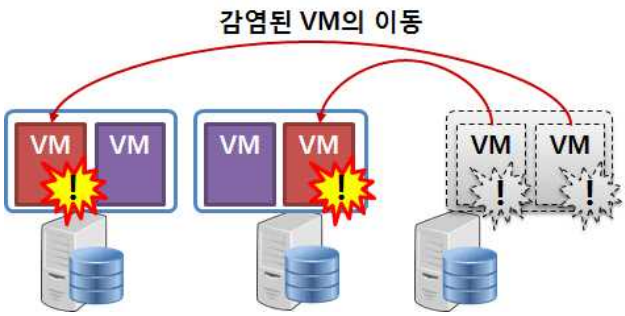
[그림 3-5] 공격자의 익명성에 따른 탐지 어려움

2) IPS(Intrusion Prevention System) : 침입방지 시스템, 필터링을 통해 유해트래픽을 차단
3) IDS(Intrusion Detection System) : 침입탐지 시스템, 악의적인 시스템 조작을 탐지

○ **(가상머신의 이동성으로 인한 문제)** 가상화 환경에서는 물리적 플랫폼 간 가상머신의 이동 (vMotion)이 용이하고 이로 인한 감염의 확산 문제 발생

- 악성코드가 감염된 가상머신, 보안패치가 안된 가상머신이 다른 물리적 플랫폼으로 쉽게 전파 가능

* 다른 물리적 서버에 가상 머신을 이동시켜주는 실시간 라이브 마이그레이션(Live Migration)을 통해 악성코드가 물리적으로 분리된 플랫폼 간에도 이동 가능



[그림 3-6] 가상머신 간 이동성으로 인한 보안 취약성

3.3. 기술외적 측면의 위협

□ **(관리측면 문제)** 관리측면의 문제는 클라우드 컴퓨팅을 서비스 하거나 도입함에 따라 파생되는 대표적인 기술외적인 보안 문제

○ **(내부자 문제)** 내부자의 실수에 의한 데이터 손실·유출이나 악의적인 의도를 가지고 데이터를 파괴 또는 탈취 하는 보안 위협

* 실제 클라우드 보안관련 사고 중 악의적인 내부자 문제가 다수 존재함(<표2-3> 참조)

○ **(해커들의 타겟)** 클라우드에 중요 정보들이 담겨 있고*, 공격 범위를 쉽게 확대가 가능하여** 얻을 수 있는 이득이 많기 때문에 고도화된 수법을 이용해 클라우드 해킹을 시도할 가능성 상존

* 클라우드가 확산하면서 기업과 개인은 중요 정보들을 클라우드에 보관하는 경향 증가, 이러한 경향은 사물인터넷과 빅데이터 확산으로 가중

* 클라우드 서버를 악성 공격에 감염시킨다면 클라우드에 접속하는 사용자들을 쉽게 감염시킬 수 있음

○ **(피해 규모의 확산)** 클라우드는 파일을 다른 사용자와 공유할 수 있기

때문에 사용자가 악성 감염 파일을 클라우드 서버에 올린다면, 피해 발생 시 규모가 커질 가능성 존재

* 사용자 기기들은 상대적으로 악성코드에 취약, 서버와 달리 백신보안이 전부인 경우가 많음

□ **(법·제도적 문제)** 클라우드가 구성된 요소의 법적, 정치적, 지리적 이유에 의해 달라지는 정책과 자원 통제력에 대한 문제

○ 클라우드는 사업자, 이용자, 제3자 등 다양한 주체들이 존재하여 서로 다양한 계약과 정책에 의해 운영

- 클라우드는 여러 국가를 거쳐 서비스를 제공할 수 있는데, 국가별 법률과 준법감시의 기준이 상이하고 클라우드의 변화에 비해 법률의 적응속도가 상대적으로 느릴 수 있음

- 보안 문제가 발생하였을 때, 데이터가 흩어져 있는 클라우드 특성상 디지털 증거를 확보하기 위한 분석방법이 필요할 수 있고, 사건을 해결하기 위한 비용이 발생할 경우 비용 책임의 문제가 있을 수 있음

4. 다양한 클라우드 보안책

4.1. 기술적인 보안책

□ **(클라우드 보안 전략)** 공유 자원의 사용으로 새롭게 야기되는 위협에 대해 기존의 보안 방식의 재구성을 통한 방어체계 구축

○ **(전송 데이터의 보호)** 인터넷으로 사용자의 데이터를 클라우드 서버에 전송할 때 발생할 수 있는 보안문제에 대해 TLS[4], SSH[5], VPN[6]을 혼합 사용함으로써 해결

- 클라우드 서비스가 SaaS나 PaaS의 경우 통신 프로토콜로 HTTP[7]를 활용하는 경우가 많은데, 이때 기본적으로 제공되는 TLS를 이용하여 네트워크 트래픽의 보안성을 유지

  * IaaS의 경우 스위치(Switch)나 라우터(Router) 레벨에서 제공되는 VPN을 활용하고 SSH의 방식도 활용하여 보안성을 강화 할 수 있음

○ **(데이터의 저장)** 클라우드 스토리지는 사용자의 데이터가 저장되는 시스템으로 저장 데이터에 대한 암호화를 활용

- 클라우드의 서비스 별로 저장되는 데이터는 상이하며, 데이터의 민감도와 공유여부, 규제 대상 여부를 고려하여 암호화 및 격실조치

  * SaaS는 문서, 사진 등, PaaS는 프로그램의 데이터를 저장하기 위한 DB, IaaS는 사용자의 VM 및 네트워크 설정 등과 같은 시스템 데이터

- 암호화는 사용자 개별단위로 이루어지며, 최소한 AES-256[8]과 같은 산업 표준 대칭 암호화 알고리즘을 활용하는 방식으로 보안성을 확보

---

4) TLS(Transport Layer Security) : 네트워크의 전송계층에서 보장하는 보안으로 SSL(Secure Sockets Layer)로도 알려져 있으며, HTTP와 같은 프로토콜에서 지원함. 인증서를 통해 상대방을 인증하고 기밀성과 무결성을 보장

5) SSH(Secure Shell) : 원격 접속을 안전하게 해주는 프로토콜로 두 호스트간의 암호화된 통신을 통해 사용자를 인증

6) VPN(Virtual Private Network) : 가상사설망, 가장 일반적인 네트워크 보안 솔루션중 하나로 두 지점의 네트워크 통신을 송수신지 정보를 캡슐화(Incapsulation)한 패킷을 이용한 터널링(Tunneling)을 통해 제공

7) HTTP(Hypertext transfer protocol) : 인터넷 상에서 HTML 문서를 교환하기 위해 사용하는 통신규약으로 웹브라우저와 같은 응용프로그램 상에서 홈페이지 주소의 통신처리 방식을 의미

8) AES-256(Advanced Encryption Standard) : 256bit의 키 길이를 갖는 AES 암호화 알고리즘으로 가장 보편적으로 많이 쓰이는 현 미국 표준 방식

- 데이터의 유실을 방지하기 위한 방법으로 DLP[9]정책의 일환으로 네트워크 단에서 외부 트래픽을 모니터링 하고 차단하는 방식을 활용

TNO 철학

- TNO(Trust No One) 방식은 데이터의 완벽한 보안을 추구하는 것으로, 해커는 물론 클라우드 서비스 업체의 직원까지도 데이터의 접근도 불허함
  - 클라우드 서비스 제공 업체가 사용자의 암호 키를 보관하는 경우 해커뿐 아니라 업체직원까지도 사용자의 데이터에 접근이 불가
  - TNO를 채택한 Lastpass 라는 SaaS 비밀번호 관리 제품은 사용자가 저장하는 로그인 정보를 기밀로 관리하며, 사용자의 키와 키에 대한 정보를 서버에 보내지 않아 내부직원 등 인적경로를 통한 유출을 원천적으로 차단함
    ※ 사용자는 마스터 암호를 활용하고 이 암호는 원본 메시지에 임의의 문자열을 추가하는 과정을 거쳐 SHA-256[10] 암호 알고리즘을 5천 번 반복하여 해시를 얻어낸 후 이 해시 값을 통해 사용자를 인증

○ **(접근 및 인증)** FIdM[11]을 활용한 사용자의 ID 인증을 통해 클라우드 접속 사용자를 인증

- 현재의 휴대폰 인증번호 입력과 유사한 개념으로 클라우드 상에서 ID관리의 어려움을 효과적으로 줄여줌
- 또한, 보안 사고에 대비하여 로그데이터를 분리된 SIEM[12]에 전송함으로써 효과적인 대응을 모색

* 시스템 로그데이터의 분석은 보안사고 발생 시 대응하기 위한 가장 기본적인 방법으로, 사용자의 로그인 및 VM의 생성·이동·소멸, 발생시킨 데이터 트래픽, 사용한 응용프로그램, DB접근, OS 및 시스템 동작 정보 등을 기록

○ **(VM간 독립성)** 공유 저장소 및 공유 네트워크에 대한 위협에 대하여 VM의 가상네트워크 보안 장점을 최대한 활용함으로써 시스템을 보호

9) DLP(Data Loss Prevention) : 전송 데이터의 형식을 탐지해 외부유출 및 유실을 막기 위한 방지 정책
10) SHA-256은 단방향 암호 알고리즘으로 암호화는 가능하지만 암호문을 복호화 하는 것은 불가능한 암호기법, 주로 패스워드에 사용하며 암호화된 패스워드가 해킹당하더라도 복호가 불가능하여 보안성을 유지
11) FIdM(Federated Identity Management) : ID 정보를 만들어 복수의 시스템과 신뢰할 수 있는 도메인에 공유하는 수단으로 사용자의 ID를 제3의 인증기관에서 인증하도록 함
12) SIEM(Security Information and Event Management) : 통합보안관제시스템, 빅데이터 수준의 장시간 심층 분석 솔루션으로 ArcSight(HP), Qrader(IBM)등이 있음

- 사용자가 접근하는 VM간의 완벽한 독립성(Isolation)을 제공하여 클라우드 환경 내에서 다른 VM의 데이터와 트래픽을 도청하지 못하게 함

  * 하이퍼바이저로 가상머신들의 물리 자원에 대한 접근권한의 범위를 제한

- 데이터는 암호화한 형태로 저장하고, 추후 삭제하더라고 저장소 어딘가에 남아있을 데이터에 대한 열람은 불가하도록 조치

- 네트워크 트래픽에 대해서는 약간의 성능 저하를 감수하더라도 앞서 언급한 TLS, SSH, VPN을 통합 활용

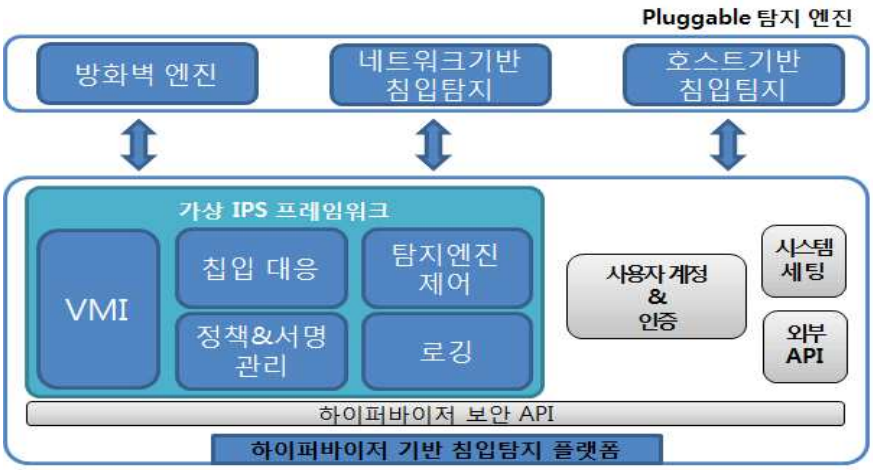
○ **(침입 탐지)** 가상머신 내부정보 분석(VMI, Virtual Machine Introspection) 기반 침입 탐지

①(하이퍼바이저 방식 탐지) 하이퍼바이저를 통해서 각 가상머신의 내부 상태를 분석하고 침입을 탐지하는 기법

- 가상머신의 vCPU(가상 CPU) 레지스터, vMem(가상 메모리)의 내용, 파일 I/O(Input Output)활동, 각 VM들이 발생시키는 네트워크 패킷 캡쳐와 같은 내부 정보에 대한 분석을 통해 악성행위 탐지

- 하이퍼바이저상에서 IPS 기능 및 방화벽, 안티바이러스 등의 서비스를 제공

  * 상용 하이퍼바이저 제작사의 VMI기반 침입탐지 기능 탑재 사례:
    · VMware사의 ESXi(VMI API(VMware, 2014)를 파트너 사들에게 제공),
    · Juniper Networks 사의 FireFly Host(Juniper Networks, 2014),
    · TrendMicro 사의 Deep Security(Trend Micro, 2014)



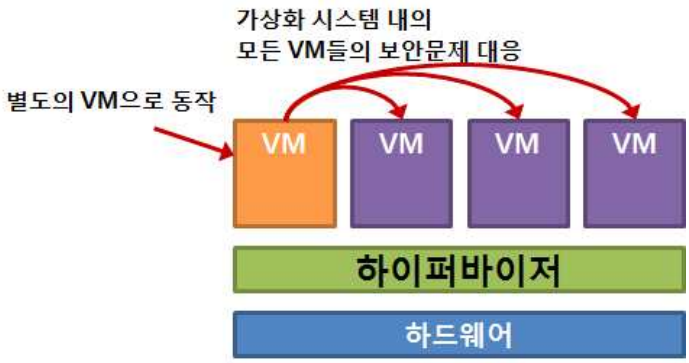
※자료 : Shin et. al. Design of a Versatile Hypervisor based Platform for Virtual Network-Host Intrusion Prevention, 2014. (재편집)

[그림 4-1] VMI 기반 침입탐지 시스템 (Xen 기반의 사례)

②(VM 방식 탐지) 에이전트리스(Agentless) 가상 보안 탐지기법

- 각 가상머신 내에서 에이전트 방식으로 동작하지 않고 별도의 특별한 권한을 가진 보안 전용의 가상머신 상에서 동작

* 에이전트 방식은 각 VM의 게스트 OS에서 실행되는 백신 에이전트를 설치하여 위협을 감시하는 방식이며, 에이전트리스는 특별한 권한을 갖는 VM이 에이전트 역할을 수행하며 이웃 VM을 감시 및 보안문제에 대응함으로써, 복수개의 도구를 관리해야하는 부담이 적음



[그림 4-2] Agentless 가상 보안 시스템

○ **(어플리케이션 보안)** 클라우드와 같은 공유 환경에서 동작하는 응용 프로그램에 대해서는 설계 시 종합적인 위협요소를 고려하여 설계

* 특히, 외부로 노출된 API를 필수적으로 사용하는 경우 기존의 보안툴과 정책을 활용하여 보안을 강화해야 하며 상황에 맞춘 설계가 필요

4.2. 기술외적인 보안책

□ **(보안 인증체계)** 클라우드 보안 인증체계를 통한 보안 표준 준수

○ ITU-T[13]와 ISO/IEC JTC 1[14]을 중심으로 한 국제 공적 표준기구에서 클라우드 보안인증 서비스를 제공

* 보안인증을 받았다는 것은 클라우드 서비스를 이용하기 위한 최소한의 정보보호 요건을 충족했으며, 보안사고가 발생하더라도 피해를 최소화 할 수 있다는 의미

* 국내에서는 한국인터넷진흥원에서 '클라우드서비스 보안평가·인증 서비스'를 제공

13) ITU-T(International Telecommunications Union Telecommunication) : 국제전기통신연합 표준화부문
14) ISO/IEC JTC 1(International Organization for Standardization/International Electro-technical Commission Joint Technical Committee 1) : 국제표준화기구(ISO)와 국제전기표준회의(IEC)의 합동 기술위원회

<표 4-1> 클라우드 보안관련 국제 표준

구분	표준	내용
정보보안	ISO/IEC 27001, 27002,	▪ 국제표준기구의 정보보호 관리체계에 대한 국제표준이자 권위있는 인증으로 클라우드 보안에 대한 산업표준도 제시 ▪ 정보보호, 통신, 운영, 접근통제, 정보 보호사고 대응에 대한 항목 평가 하며, 매년 감사 및 표준준수 여부 시행
	ISO/IEC 27018	▪ 클라우드에 저장 된 민감한 고객정보(특히 개인식별정보)의 보호, 보안 리스크 실행방안의 평가 및 가이드라인
보안제어	SOC (SOC1, SOC2)	▪ SOC는 미국공인회계사협회(AICPA)에서 발급하는 인증체계로 재무정보에 대한 규제 - (SOC 1) 기업의 재무 보고를 위한 정보 및 관리 시스템 등 종합적인 내부통제를 평가하는 인증 - (SOC 2) 개인정보보호 시스템, 조직/관리시스템 등 기업의 내부통제를 평가하는 인증으로 클라우드 서비스, 데이터 센터 등의 출현으로 서비스 인증 체계가 마련
정부 및 산업 표준	FedRAMP/FISMA	▪ 미국 연방정보보안 관리법으로 정부 정보시스템의 보안 강화를 위해 정부 정보보안개혁법과 이를 승계한 연방정보보안 관리법을 통해 적정 보안조치를 취하지 않은 부처는 예산을 삭감토록 해 강력한 정책 집행의 기반을 마련

※참고 : MS, Compliance, 2015.
※주 : 상기 표준 외 다수

□ **(보상 및 보험)** 클라우드 보안사고 발생 시 보상하는 제도 및 보험을 통한 사고대응 방안 존재

○ 클라우드 SLA[15]를 통해 데이터보호, 계정관리, 어플리케이션 운용 등 서비스 레벨 관리에 대한 약정을 진행

* 클라우드 서비스 제공업체가 사용자에게 서비스의 수준을 정량화하여 명확히 공지하고, 미달할 경우 손해를 배상하도록 하여 서비스의 품질을 보장하기 위한 약정

* 글로벌 기업의 경우 보안피해 발생 시 사용량에 따라 10~50%까지 이용요금을 배상하며 국내의 경우 3~15% 및 장애발생시간동안 과금액의 3배에 해당하는 비용을 보상 (아마존 AWS의 경우, 월 사용료의 10% 정도의 보상금을 지급)

○ 클라우드 보험을 통한 보상 서비스의 제공

- SK텔레콤은 삼성화재와 협력하여 클라우드 보험 서비스인 ‘T클라우드 비즈’와 사용자들을 위한 ‘이비즈 배상책임보험’ 계약을 체결

* 보험 가입자가 시스템 오류, 네트워크 접속 불가 등 예상치 못한 서비스 중단으로 금전적

15) SLA(Service Level Agreement) : 서비스 수준 협약서, 서비스 공급자와 사용자간의 공식적으로 합의된 협의서

피해를 입었을 경우 최대 10억 원까지 보상금을 지급하며, 웜 바이러스를 제외한 해킹에 의한 영업 손실도 보상

- 이 밖에도 클라우드 서비스 업체인 호스트웨이(4시간 이상 장애시 시간당 평균요금의 5배 보상), 스마일서브(1시간 이상 장애시 하루 사용료 감면), 카페24(호스트웨이와 동일) 등도 서비스 장애에 대한 보상금 지급

□ **(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 안정성 보장

지리적 분산 도구로써의 클라우드

- 데이터와 기능을 클라우드로 옮기는 것 자체는 보안상의 위험을 내포하고 있지만, 역설적으로 클라우드는 보안 도구로써의 가치도 지님

※ 단일접점의 취약성 : 사용자의 모든 디바이스들과 클라우드 계정이 연결되어 단일화 시키는 것에 대한 위험성이 존재하며 공격의 빌미를 제공

- 클라우드 컴퓨팅은 한곳에서 고장이 발생할 경우의 위험을 완화

※ 지리적 분산 : 재난 및 재해, 화재, 통신중단 등의 위협에서 지리적으로 분산된 데이터 센터는 효율적인 대응책이 될 수 있으며, 다수의 분산된 데이터 센터는 사용자의 상대적으로 근거리에 위치한 접속을 허용함으로써 원격 통신에 의한 네트워크 지연을 줄여줄 수 있음

※ 플랫폼 분산 : 사이버 공격이 특정 클라우드 어플리케이션을 대상으로 할 때, 서로 다른 방식의 프로토콜 및 시스템 운영체제는 한 번의 공격으로 양쪽이 뚫리는 위험을 방지

※ 인프라 분산 : 클라우드 시스템의 하드웨어 및 네트워크 환경이 다른 방식으로 운영된다는 것은 보안 취약점이 분산되는 이점도 존재

5. 요약과 시사

가. 클라우드 보안 문제에 대한 해결책

□ 클라우드 시스템에서의 보안은 기업 및 기관의 클라우드 도입을 저해하는 불안 요소이며, 클라우드의 다양한 보안 문제에 대한 기술·기술외적인 보안책은 다양하게 존재

○ 클라우드는 기본적으로 일반적인 시스템의 보안과 같은 문제를 가지고 있으며 해결 방안도 기본적으로 유사

○ 다만, 가상화 기술로 인한 공유자원 환경으로 인해 더 복합적으로 보안을 고려해야 하나 이는 기존의 보안 방식을 재구성한 방어체계로 해결 가능

<표 5-1> 클라우드 보안 문제와 해결책 정리

구분	위협요소		해결방안
기술적	기존 보안 위협 상속	▪ 네트워크 트래픽의 도청 및 위변조 ▪ 인증 및 접근권한 탈취에 따른 데이터 유출·손실 ▪ 서비스 거부(DoS, DDoS) 공격 ▪ 시스템 설계상의 오류	▪ 암호화, 해싱, 디지털 서명, 중복 모니터링 등 강화 - 데이터 송수신 암호화 - 저장된 데이터의 암호화 및 키관리 - 주기적 백업 및 백신 관리 - 다단계 인증 및 접속 관리
	가상화를 통한 위협	▪ 하이퍼바이저 감염 ▪ VM내부공격 용이성 ▪ 공격자 익명성 ▪ 가상머신의 이동성에 따른 보안 문제	▪ 암호화를 통한 전송데이터의 보호 ▪ 저장 데이터에 대한 암호화 및 키 관리 ▪ 접근 권한에 대한 해쉬 검사 ▪ 자원사용량 제한, 로그이력관리 등 VM간의 독립성 보장 ▪ 다양한 침입탐지 기법의 도입 - 하이퍼바이저 기반의 VM감시·대응 - 에이전트리스 기반 VM감시·대응 ▪ 보안사항을 고려한 프로그램 설계
기술외적	관리측면 문제	▪ 내부자 문제 ▪ 해커들의 타겟 ▪ 피해규모의 확산 ▪ 물리적인 저장소 관리 ▪ 자연재해	▪ 내부자들에 대한 교육 및 검증된 채용 ▪ 국제 클라우드 보안 표준을 준수하는 인증 획득 ▪ 보안 사고발생시 보상하는 제도 및 보험을 통한 사고 대응
	법제도 문제	▪ 국가별 상이한 법체계	▪ 법적인 쟁점을 사전 점검 후 시스템 설계·도입 ▪ 국제 표준

나. 보안 이슈에 대한 고찰

□ 기본적으로 어떤 하드웨어나 소프트웨어도 보안 위협에는 항상 노출되어 있으며, 보안 문제는 컴퓨터 시스템이 존재하는 한 끊임없이 고려해야할 문제

○ 해커들의 공격 유형은 오늘날까지 계속 진화해 왔고, 그에 맞춰 보안 기술들도 발전해 왔음

- 모든 시스템의 100% 완벽한 보안은 보장할 수 있는 것이 아니며, 컴퓨터 시스템의 보안은 100%에 가깝도록 발전해 나가는 것

- 따라서, **'완벽한 보안'** 보다는 **'피해의 방지 및 최소화'**에 초점을 맞추는 것이 현실적인 답이라 할 수 있음

□ 클라우드 보안 문제를 해결하기 위한 다양한 **기술적 솔루션**들이 현재 존재하며, **인증 및 보험등과 같은 기술외적인 해결책**도 존재

○ 특히, 기술적인 부분의 보안 솔루션은 현재도 많은 시스템에 사용되면서 위협을 방지하고, 새로운 위협이 등장할 때마다 발전하고 있음

○ 기술 외적인 부분의 문제는 제도적인 해결책이나 인식의 전환으로 풀어하는 문제

- 인증 제도의 강화, 클라우드 서비스 제공업체의 내부자 교육 및 관리 시스템 개선, 법적인 사전 검토, 사용자의 보안 인식 확대로 인한 철저한 계정관리 등이 필요

□ 결론적으로, 다양한 클라우드 보안 솔루션들로 인해 **클라우드의 보안은 일반적인 정보보안 수준 이상**으로 이루어지고 있으며, 도입 및 활용에 있어서 심각한 우려사항은 아니라고 판단됨

* 실제 MS, 시만텍 같은 클라우드 서비스 업체 및 관련 업체들은 자체적인 보안 솔루션을 출시하며 클라우드 서비스의 보안성을 강화하고 있음 ([부록 4]참조)

○ 클라우드는 다양한 활용측면 및 비용 절감 등의 장점이 크기에, 앞으로도 더 안전한 활용을 위한 다양한 보안 솔루션들이 등장할 것

그 외 클라우드 활성화를 위한 노력

- (보안측면) 보안인증 및 이용자 보호제도의 강화를 통해 클라우드 보안수준 보장하며 사고 발생 시 즉각적인 대응으로 피해를 최소화할 수 있는 방안의 마련
  - (정부) 안전성 및 신뢰성 검증을 위한 클라우드 보안인증 제도의 도입을 통한 최소한의 기준 마련하고 이용자 보호제도를 통해 보안사고 발생 시 피해를 최소화
    ※ 과기정통부와 한국인터넷진흥원은 '클라우드 컴퓨팅 서비스 보안 인증제도'를 추진 중 (2017.7)
  - (서비스 업체) 클라우드 서비스 업체는 자사의 보안수준을 강화하고 공신력 있는 인증을 획득하여 사용자에게 신뢰를 제공
  - (사용자) 클라우드 서비스 이용자는 막연한 보안 우려를 해소하는 인식 전환이 필요하며, 서비스 사용 중 스스로 정보보호를 위한 최소한의 노력을 기울여야 함
    ※ 'K-ICT 클라우드 컴퓨팅 활성화 시행계획(과기정통부 2017)'을 통한 대국민 인식 확산 추진
- (기타) 정부의 다양한 정책적 노력에도 불구하고 국내의 클라우드 확산이 느린 원인에 대한 다각화된 진단도 병행해야 함 ([부록 5] 참조)
  ※ 보안문제를 제외하고 클라우드 확산이 미비한 원인은 도입 비용부담의 측면, 시장변화 대응 및 원천기술의 부족, 제도적 미비점 등으로 조사 ([부록 6] 참조)

[부록 1] 클라우드 컴퓨팅의 분류

□ 서비스 제공방식(SaaS, PaaS, IaaS), 구현방법 및 구성유형(Public, Private, Hybrid), 활용대상(B2B, B2C, B2G)에 따라 분류

<표 a> 클라우드 컴퓨팅 분류

구분	모델	정의	특징 및 활용
서비스 모델	IaaS	(Infrastructure as a Service)클라우드 서비스가 가능하기 위해 필요한 기반인 인프라에 관한 서비스	가상화(Virtualization) 및 네트워크 기술을 통해 여러 물리적인 컴퓨팅 자원을 분할, 통합, 관리하는 가상 머신(Virtual Machine) 환경서비스 제공 ※예: 아마존 AWS, KT, LGCNS, SK 등
	PaaS	(Platform as a Service)플랫폼 제공 형태의 서비스	개발자들에게 개발을 위한 도구로써 표준, 개발응용 프로그램의 배포를 위한 채널 등을 제공 ※예: 구글의 APP엔진 등
	SaaS	(Software as a Service)클라우드 인프라 및 플랫폼 상에서 구동하는 온디맨드(On-Demand) 형태의 응용 소프트웨어와 데이터베이스 등을 제공하는 서비스	사용자가 별도의 응용프로그램을 설치할 필요 없이 서비스를 제공받고, 프로그램의 관리 및 유지보수 등과 같은 추가적 비용 불필요 ※예: 구글 Docs, 네이버 클라우드, Dropbox, MS오피스, 한컴오피스 등
배치 방식	Public	누구나 인터넷을 통해 클라우드 제공 사업자의 서비스 사용 가능	비용절감, 협업의 용이성 등이 장점
	Private	특정 조직만이 클라우드 컴퓨팅을 사용할 수 있도록 구축하는 서비스	초기 투자비용은 높으나 보안과 안정성이 높음
	Hybrid	Public과 Private 클라우드의 혼합된 형태의 서비스	보안이 낮은 업무는 Public, 보안이 높은 업무는 Private 클라우드를 활용
활용 대상	B2B	(Business to business)기업이 활용하는 업무용 클라우드 컴퓨팅 모델	ERP, CRM, SCM, 오피스 등 업무용 클라우드 활용
	B2C	(Business to customer)개인이 활용하는 클라우드 컴퓨팅 모델	오피스, 네이버 클라우드 등 개인 자료 저장 등 활용
	B2G	(Business to government)공공기관이 활용하는 클라우드 컴퓨팅 모델	(미국)민간기업의 클라우드 컴퓨팅 활용 (한국)Private 클라우드 구축

※자료 : NIST(미 국립표준기술연구소), 2011.
정보통신산업진흥원, 클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률 설명자료, 2013.

○ 클라우드는 제공하는 서비스(가상인프라, 플랫폼, 응용소프트웨어)에 따라 벤더의 관리범위도 나뉠 수 있으며, 확보해야 하는 보안 전략도 상이할 수 있음

- 인프라를 서비스로 제공하는 경우 하드웨어(서버, 스토리지, 네트워크) 상의 보안과 해당 하드웨어를 구동하기 위한 시스템 소프트웨어, 서버 등의 단말 가상화 측면의 보안 이슈가 주류

- 플랫폼을 서비스로 제공하는 경우에는 시스템 소프트웨어 및 가상환경에서 공유된 리소스 관리 측면, 설계상의 취약점, 계정에 대한 인증 차원의 보안 이슈가 있음

- 응용프로그램 등을 서비스로 제공하는 경우에는 인프라와 플랫폼의 보안이 보장된다는 가정 하에 서비스를 왜곡하거나 해커의 의도에 따른 위협으로 유도, 서비스의 거부 등의 이슈가 존재

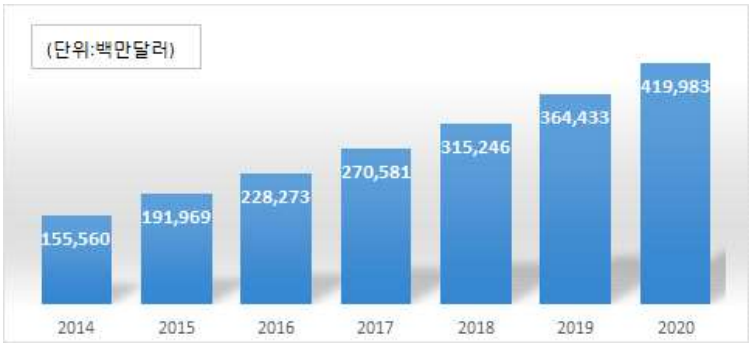
※세부 이미지 출처 : 위키미디어, 클라우드 컴퓨팅 (재편집)

[그림 a] 클라우드 컴퓨팅 구분 별 요소

[부록 2] 클라우드 컴퓨팅의 가속화

□ (시장성장) 글로벌 클라우드 컴퓨팅 시장은 2017년 2,706억 달러에서 2020년 4,200억 달러 가까이 성장 할 것으로 전망

* 퍼블릭 클라우드 시장 또한 2020년 까지 1,950억 달러에 이를 전망(IDC 2016)

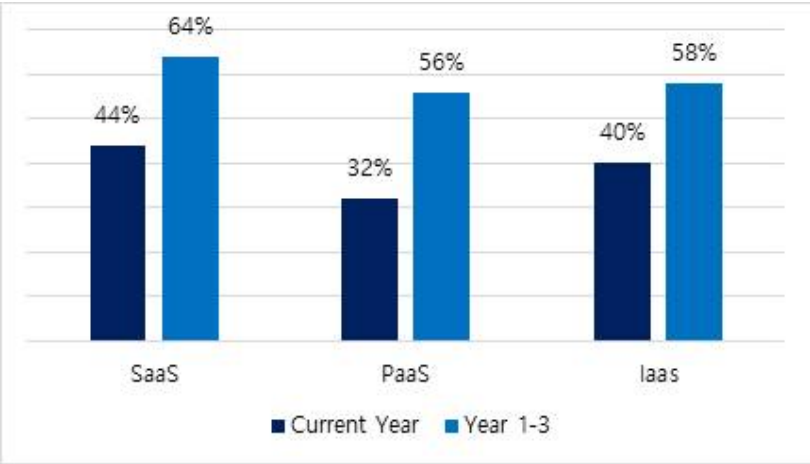


※자료 : Gartner 2016

[그림 a] 클라우드 세계시장 규모

○ 반면, 국내의 클라우드 컴퓨팅 시장은 2020년까지 64억 달러(한화 약 7조 3천억 원) 규모로 성장할 것으로 예상 되지만, **세계 규모 대비 0.6%에 불과**

□ (투자규모 확산) 글로벌 IT 기업들의 투자 규모 또한 큰 비율로 증가하여 2016년 기준 각각 44%(SaaS), 32%(PaaS), 40%(IaaS) 수준의 투자를 향후 1~3년 내에 각각 64%, 56%, 58%로 늘릴 것으로 조사



※자료 : KPMG, Journey to the cloud, 2017.

[그림 b] 향후 1~3년 이내 클라우드 투자 규모 변화

글로벌 클라우드 컴퓨팅 확산 사례

- 대표적인 패키지SW 기업인 MS, IBM, 오라클 등은 모두 클라우드 컴퓨팅 서비스를 제공하고 있으며 클라우드 컴퓨팅에 적극 투자를 진행
  - IBM의 경우 2014년 클라우드 컴퓨팅 투자 규모는 약 12억 달러였으며, 2015년부터 이후 4년간 30억불을 투자할 계획을 가지고 투자개발을 진행
  - 오라클은 자사 SW를 클라우드 컴퓨팅으로 서비스(월 175달러)하여 지난 2015년에만 20억 달러의 매출을 달성
- 제조업, 금융업, 의료업 및 새롭게 등장하는 AI 등 산업전반에 걸쳐 클라우드 컴퓨팅이 적용되어 그 중요성은 점차 증가
  - GE 등 글로벌 제조업체 또한 클라우드 컴퓨팅을 직접 개발 및 산업에 적용하여 산업 혁신을 가속화
  - GE는 산업 기계 및 설비에서 발생하는 데이터를 수집·분석하여, 산업용 SaaS를 개발하고 제공하는 PaaS인 Predix Cloud를 출시
  - 또한, 지난 2016년 3월 국민적 반향을 일으켰던 구글의 알파고나 제퍼디 퀴즈쇼에서 우승한 바 있는 IBM의 왓슨 등의 인공지능은 모두 클라우드 컴퓨팅 기반을 통해 구현

[부록 3] 클라우드 보안위협요소에 대한 다양한 정의 및 재분류

□ 클라우드 및 보안 관련한 각 기관과 학회 등은 클라우드 서비스의 보안 위협요소에 대하여 다양하게 정의하고 있음

○ 보안공학회 논문지(정성재 2013)에서는 크게 6가지의 클라우드 서비스에 대한 보안 위협 요소를 분류했으며 이는 기술·기술외적 문제로 분류 가능

<표 a> '보안공학회지 클라우드 서비스의 핵심 보안 위협요소'와 재분류

보안위협	위협내용	구분
가상화 취약점 상속	▪ 악성코드 감염 및 확산위협 ▪ 서비스 가용성 침해	기술적 문제
자원공유 및 집중화에 따른 서비스 장애	▪ 시스템 장애 시 모든 고객의 서비스 중단 ▪ 중앙시스템 노출 시 DDoS(Distributed Denial of Service)등의 공격대상이 되기 쉬움	
분산처리에 따른 보안적용의 어려움	▪ 자원공유와 가상머신 동적 재배치로 인증/접근제어 복잡도 상승 ▪ 분산 컴퓨팅 시스템에 일괄적인 인증/접근제어 적용의 어려움	
정보위탁에 따른 정보유출의 위협	▪ 소유와 관리 분리에 따른 정보유출 ▪ 내부자에 의한 정보유출	기술외적 문제
사용 단말의 다양성과 분실에 따른 정보유출	▪ 단말기 분실 등에 의한 정보유출	
법규 및 규제의 문제	▪ 정보유출 시 책임소재 불분명 ▪ 자원공유에 따라 감사증적이 어려움	

※자료 : HJ Lee, Security Consieration for use of Secure Cloud Services, CloudSec 2012, 정성재 외, 클라우드 보안 위협요소와 기술 동향 분석, 보안공학연구논문지, 2013 (재편집)

○ CSA(Cloud Security Alliance)에서는 가장 최신의 분류 기준으로 보안 위협요소를 12가지*로 정의했으며 정의한 문제의 대부분은 기술적 문제보다 기술외적(사람)인 문제를 지적

* CSA는 기술적인 위협대응책이 있어도 내부 인력에 의해 의도된 위협은 막기 어려우며, 내부자 보안 인식 교육이 클라우드 서비스 보안을 위해서는 매우 중요한 요소임을 지적

- <표 b>에 나타난 바와 같이, 순수 기술적인 문제로 불거질 수 있는 보안 문제는 시스템 취약성, 지능형 지속공격, 분산 서비스 거부 공격이며, 기술외적인 문제는 주로 불충분한 관리와 부주의, 내부자의 도덕적 해이 등이 주원인으로 파악

- 기술·기술외적인 요인 둘 모두에 해당될 수 있는 문제는 기존 보안 위협 및 클라우드의 특성으로 인한 위협에 관리 문제가 복합된 형태

* 기술과 기술외적 복합요인에 해당되는 보안 위협들은 서비스 사업자나 이용자의 실수를 줄이고 시스템을 얼마나 주의 깊게 관리하는 가에 따라 위협을 예방할 수 있음을 시사

<표 b> 'CSA의 클라우드 서비스 핵심 보안위협요소'에 대한 원인분석 및 재분류

구 분		주요 내용	원 인	비고
1	데이터 유출	▪ 민감한 정보, 보호된 정보에 대한 유출 ▪ 민감도에 따른 손상율 상이	▪ 기술적 해킹에 의한 유출 ▪ 관리실수에 의한 유출	◐
2	신분 및 접근에 대한 불충분한 관리	▪ 암호 키가 본문에 포함되거나 약한 비밀번호의 사용 ▪ 작업종료 또는 무응답에 대한 빠른 세션 종료의 부재	▪ 비밀번호 도난 등 사용자의 약한 보안관리 ▪ 시스템 설계상의 문제	●
3	안전하지 않은 인터페이스와 애플리케이션 프로그래밍	▪ 애플리케이션 구축을 서두르기 위해서 기존의 코드를 재사용하거나 합성해서 사용하면 보안에 위협	▪ 시스템 구축 단계에서 발생할 수 있는 문제로 사업자의 충분한 단속과 검토가 필요	●
4	시스템 취약점	▪ 공격자가 프로그램에 악용할 수 있는 기술적인 버그	▪ 컴퓨터 발명 이후 현재까지 위협이 될 수 있는 기술 문제	○
5	계정 및 서비스 하이재킹	▪ 피싱이나 사기 등 각종 악성 사이트로 유도(redirection) 하여 계정 등을 탈취	▪ 피싱, 파밍의 유도	◐
6	악의적인 내부 관계자	▪ 시스템 접근 권한을 갖는 내부자의 위협 ▪ 도덕적으로 적합하지 않은 사람의 고용	▪ 클라우드 서비스 사업체 내부 직원의 도덕성	●
7	지능형 지속공격 (APT)	▪ 시스템에 침투하여 기밀정보를 탈취하거나 파괴	▪ 루트킷, 백도어, 웹바이러스 등의 침입	○
8	데이터의 유실	▪ 악의적인 공격 외에 클라우드에 저장된 데이터의 유실	▪ 관리자의 우발적인 삭제 ▪ 화재,지진 등의 물리적 재앙으로 인한 파괴 ▪ 암호화 키의 분실	●
9	불충분한 실사	▪ 클라우드 사업시 충분한 실사와 재정, 기술,법적 검토 없이 도입	▪ 사업자의 부주의	●
10	클라우드 컴퓨팅 남용 및 불손한 사용	▪ 악의적인 의도를 가진 사업자의 클라우드 도입, 더 찾아내기 힘들고 위험한 존재가 될 수 있음	▪ 클라우드 서비스 사업체의 도덕성	●
11	분산 서비스 거부 공격	▪ 여러 대의 공격자를 분산 배치하여 동시에 특정 사이트를 공격	▪ DoS, DDoS 등의 공격	○
12	공유 기술의 취약점	▪ 가상 머신을 적절히 관리하지 못하면, 하나의 작은 구멍으로 전체가 위협받을 가능성	▪ 관리의 문제 ▪ 기술적 취약성	◐

※참고 : CSA, Cloud computing top threats in 2016, 2016. (재편집)
※편집 주 : 기술적요인(○), 기술외적요인(●), 기술 및 기술외적요인(◐)

○ NIST(미 표준기술연구소), Gartner, UC Berkeley등도 각각 클라우드의 위협 요소를 8, 7, 10 가지 요소로 나누어 정의하고 있으며, 대부분의 내용은 유사함

<표 c> 그 외 기관들의 클라우드 보안 위협 분류

구분	분류 내용
NIST (클라우드 고객관점 위험레벨 8가지)	▪ 관리부재, 고립의 어려움, 서비스 제공자 의존, 규제위협, 데이터보호, 관리 인터페이스 보완, 안전하지 않은 데이터 삭제, 악의적인 내부자
Gartner (클라우드 7가지 위협)	▪ 권한 관리자의 접근, 정책, 데이터 저장 위치, 조사자원, 데이터 분리, 복구, 장기적 생존 가능성
UC Berkeley (클라우드 10가지 보안 요소)	▪ 서비스 가용성, 데이터 Lock-In, 데이터 기밀과 감시, 데이터 전송장애 요소, 불확실한 성능 예측, 확장 가능한 스토리지, 대규모 분산 시스템 버그, 신속한 스케일링, 평판 공유, 소프트웨어 라이센싱

※자료 : 한국인터넷진흥원, 클라우드 서비스 정보보호 안내서, 2011.

○ 클라우드컴퓨팅(홍릉출판사, 2016) 에서는 클라우드 환경의 기술적인 위협 범주는 네트워크, 서비스, 가상화, 인증 및 접근 권한, 가용성, 중복된 신뢰 경계, 구현의 오류 등 총 7가지 세부 항목으로 구분

- 대부분의 위협요소는 기존의 보안 위협과 동일한 기술적 요소이며, 가상화 및 분산시스템에 따른 보안 위협 요소가 새로울 수 있으나, 기존 요소들의 융합된 형태로 존재

<표 d> '클라우드 환경의 기술적인 위협 범주'와 위협 구분

범주구분	위협의 예	위협 구분
네트워크	▪ 네트워크 트래픽 도청 ▪ 악의적인 중간자	기존의 보안 문제와 동일
서비스	▪ 서비스 정의의 왜곡 ▪ 래핑, 웹서비스언어 스캐닝 공격	기존의 보안 문제와 동일
가상화	▪ VM 탈출, VM 호핑, VM 이미지 변조 공격 ▪ 하이퍼바이저 기반 루트킷	기존 가상화 문제와 동일
인증 및 접근 권한	▪ 접근 권한의 위·변조 ▪ 식별자 관리 및 익명화	기존의 보안 문제와 동일
가용성	▪ DoS, DDoS 공격 ▪ 가상 머신의 급격한 생성	기존의 보안 문제와 동일
중복된 신뢰 경계	▪ Multi-Tenancy로 인한 보안경계의 중첩 문제	클라우드 시스템 문제
구현의 오류	▪ 설계 결함 등을 취약점으로 악용	기존의 보안 문제와 동일

※자료: 클라우드컴퓨팅-개념,기술,구축체험 ,홍릉출판사, 2016 (재편집)

[부록 4] 글로벌SW기업의 클라우드 보안 방침과 솔루션 사례

□ MS(Microsoft)의 클라우드 컴퓨팅 보안성 향상을 위한 방침

항목	내용
데이터센터 물리보안	▪ 하루 24시간 주 7일 내내(항상) 물리적인 접근의 통제 ▪ 동작 감지기, 생체정보 기반 시설 접근통제, 감시카메라 가동, 물리적 침입 탐지
네트워크	▪ 분리된 물리적 네트워크 및 암호화된 연결 ▪ 가상네트워크에도 별도의 인터넷 연결성 보장
인증과 권한통제	▪ 계정 인증과 접근 제어, 기업용 클라우드 인증, 접근 모니터링, Single sign-on, Multi-Factor Authentication, Role based access 제어
호스트보안	▪ 암호화된 데이터 전송을 통한 데이터 보호 ▪ 데이터 저장 시 암호화 옵션 및 데이터의 구분과 저장위치에 대한 선택권 부여
데이터 프라이버시	▪ 클라우드 서비스 디자인 단계에서 프라이버시 적용 ▪ 계약상의 규제 및 제한된 데이터 접근의 준수 - 계약상의 규제 : 1. EU Data Privacy Approval : EU 고객의 데이터 보호 규정, EU Data Privacy의 MS 데이터전송 허용(EU Article 29 승인) 2. 제한된 데이터 접근의 준수 : 기업의 데이터 보호에 대한 규제의 해결방안으로 제시 (규제 인증: HIPAABAA, Data Processing Agreement, & E.U. Model Clauses), - 제한된 사용과 접근 : 광고목적의 데이터 접근 차단 및 인증 없는 고객의 데이터 공유 차단

※ 자료: MS-Azure Security Center 2016.

□ 시만텍 통합 보안 솔루션 사례

○ 클라우드 시큐리티 플랫폼을 통한 클라우드 전 영역에서 정보보안 보장 및 보안 위협에 대한 보호 제공[16)]

* 데이터 유출방지 솔루션(DLP) 및 지능형 악성코드 분석 서비스(Malware Analysis Advanced Service)를 통한 강력한 웹 보안 서비스 제공

- CASB[17)]로써 AWS(아마존)와 Asure(MS)를 위한 클라우드 워크로드 프로텍션 구축

* AWS와 연동하기 위한 블루코트(Blue Coat)사의 ProxySG[18)] 기반 방화벽 구축

* Asure의 보안성 강화를 위해 사용자 활동 모니터링 및 행동 분석을 통한 계정 탈취 감지

16) ※기사참조: 보안뉴스, 시만텍, 클라우드 보안 과제 해결 위한 통합 클라우드 보안 솔루션 발표, 2017
17) CASB(Cloud Access Security Broker) : 클라우드 서비스 접속 보안 중개, 클라우드 서비스와 이용자 사이에 위치하며 독립적인 보안 기능을 수행
18) 블루코트사에서 제작한 웹 게이트웨이 솔루션으로 미 국방부에서 활용하기 위한 통합성능승인제품군(UC-APL) 인증을 받음

[부록 5] 클라우드 컴퓨팅 활성화 정책 비교

□ 클라우드 컴퓨팅을 활성화하기 위해 국내에서는 다양한 정책들을 제시하고 추진

정책	시행주체	정책의 내용 및 성과
범정부 클라우드 컴퓨팅 활성화 종합계획 (2009)	행안부, 산자부, 방통위	▪ 범정부 클라우드 사무환경 및 영상회의시스템 통합구축 (재량, 신규, 국정과제, 정보화) ▪ 범정부 클라우드 사무환경 통합구축 ▪ 영상회의시스템 구축
클라우드 컴퓨팅 확산 및 경쟁력 강화 전략 (2011)	행안부, 산자부, 방통위	▪ 글로벌 클라우드 서비스 창출을 통한 경제 활성화, 공공분야 IT 인프라의 선진화와 효율화, 믿고 안전하게 쓸 수 있는 이용환경 조성
클라우드 기반 범정부 IT거버넌스 추진계획 (2011)	행안부, 산자부, 방통위	▪ 클라우드 기반 IT자원 통합, 범정부 공통 플랫폼 구현, 스마트오피스 업무환경 구축, 대국민 서비스 고도화, 클라우드 활성화 기반 조성
클라우드 SLA가이드, 개인정보보호수칙 (2011)	방통위	▪ 클라우드 서비스의 수준이 명확히 제시되면 이용자의 클라우드에 대한 막연한 불안감 해소
클라우드 산업육성 계획 (2014)	행안부, 과기정통부	▪ 공공선도·민간확산으로 클라우드 서비스 시장 확대, 클라우드 플랫폼 확보 및 쉬운 창업환경 조성으로 산업 경쟁력 강화, 중소 클라우드 기업의 지속발전 가능한 협업 생태계 조성
클라우드 컴퓨팅 발전 및 이용자 보호에 관한 법률(2015.9),	과기정통부	▪ '클라우드 컴퓨팅 발전 및 이용자 보호에 관한 법률' 제정('15.3) 및 시행('15.9), 정보보호대책('15.9) 및 기본계획 수립('15.11) ▪ 관련 분야의 육성 및 지원 근거를 마련, 해당 산업의 발전을 저해하는 기존 규제 개선, 안전한 서비스 이용환경 조성
K-ICT 클라우드 컴퓨팅 활성화 계획(2015)	과기정통부	▪ 공공부문의 선제적인 클라우드 도입, 민간부문 클라우드 이용 확산, 클라우드 산업 성장 생태계 구축을 추진하여 2021 클라우드 선도국가 도약하는 방안 추진
클라우드 컴퓨팅 서비스 정보보호에 관한 기준 (2016)	과기정통부	▪ 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」 제23조 제2항에 따라 클라우드컴퓨팅서비스의 안전성 및 신뢰성 향상에 필요한 정보보호의 구체적인 기준 설정
공공기관 민간 클라우드 이용 가이드라인마련 (2016)	행안부	▪ 민간 클라우드 업체가 상용으로 제공하는 클라우드 컴퓨팅 서비스를 공공기관이 이용하기 위한 기준과 절차 규정 ▪ 클라우드 컴퓨팅법 시행 이후 첫번째로 진행된 '공공부문 클라우드 컴퓨팅 수요조사'에 따르면, 민간클라우드 이용 기관수는 2016년 동안 23개에서 2017년 51개로 증가했으며, 시스템은 35개에서 116개로 증가
2017년 K-ICT 클라우드컴퓨팅 활성화 시행계획 (2017)	과기정통부	▪ 국내 클라우드 시장 규모는 1.19조원으로 전년(7,664억원) 대비 55.2% 증가, 클라우드 기업도 전년 대비 51.6% 증가 (353→535개, 182개↑)

[부록 6] 국내 클라우드 확산이 미비한 원인에 대한 고찰 - 보안외적요인

□ **(도입 비용부담의 측면)** 클라우드를 사용하는 비용 부담 외에도, Private 클라우드를 구축 및 사용하는 비용 부담

* 민간 기업 48.7%, 공공기관 25%가 클라우드 도입을 위한 비용부담을 우려(정보통신산업진흥원, 클라우드산업실태조사, 2015)

○ Private 클라우드는 Public 클라우드에 비해 독립적인 시스템을 새로 구축해야하며, 일반적으로 제공 되는 서비스가 한정적이고 가격이 비쌈

* 물리적인 망 자체를 분리하는 방법도 활용되고 있으며, 이에 따라 2중망을 유지해야 하는 업무 중복성 및 비효율성 문제도 야기

○ 그 외에도, 시장변화의 대응 및 원천기술의 부족, 제도적 미비점 등도 보안 외적 요인으로 지적

□ **(시장변화 대응 및 원천기술의 부족)** 글로벌 기업은 다양한 마케팅 및 제품 기술을 바탕으로 적극적인 시장 진출

○ 특히 아마존(AWS), MS(Azure), IBM 등은 국내 시장 선점을 위해 클라우드 데이터센터를 개소하고 시장을 공략하는 추세

* 이 기업들은 자체 솔루션 보유하고 클라우드 상의 방대한 데이터로 머신러닝과 연계한 기능을 선보이며 많은 구축 경험과 노하우, 가격 경쟁력 등을 바탕으로 시장에서 경쟁우위에 있는 상황

○ 국내 통신사 및 SW업체 등이 시장 점유를 위해 노력중이며, SaaS의 경우 일부 경쟁력을 보유하고 있으나 IaaS, PaaS는 원천기술이 부족

* 클라우드 플랫폼 SW는 자원 가상화 및 통합, 데이터 저장 등의 기술 분야에서 유럽 및 일본에 좀 더 근접하고 있으나, 원천기술 개발을 위한 산업 여건, 축적된 경험, 전문 인력 확보 등의 기반 인프라가 전반적으로 선진국 대비 취약

<표 a> 클라우드 컴퓨팅 분야의 기술수준

소분류	상대수준 (%)					격차기간 (년수)				
	한	미	일	유	중	한	미	일	유	중
클라우드컴퓨팅 아키텍처	76.2	100	80.7	84.9	73.1	1.9	0.0	1.5	1.2	2.1
클라우드 자원 가상화 및 통합	77.2	100	80.2	85.0	73.0	1.7	0.0	1.4	1.1	2.0
클라우드 데이터, 저장, 분석	78.6	100	81.7	85.6	74.5	1.6	0.0	1.4	1.1	2.0
기타 클라우드컴퓨팅 기술	75.9	100	81.7	84.5	73.9	1.8	0.0	1.4	1.1	2.0

※출처: IITP, 2015년도 ICT 기술수준 조사보고서, 2016.

□ **(제도적 미비)** 정부의 클라우드 발전법 제정 및 기본계획이 수립되었으나, 클라우드 활성화를 저해하는 기존 제도 운영의 문제, 각 산업별 규제들이 여전히 존재하는 것이 현실

○ 결국, 클라우드 도입을 위한 기관별 분류 기준 등이 오히려 공공부문의 클라우드 도입 저해할 수 있다는 의견이 있음

<표 b> 정보자원 중요도에 따른 클라우드 우선 적용 원칙

대상기관	정보자원 중요도		
	상	중	하
중앙행정기관	▪ G-클라우드	▪ G-클라우드	▪ G-클라우드 우선
지자체	▪ 자체 클라우드	▪ 자체 클라우드 ▪ 민간 클라우드 검토	▪ 자체 클라우드 ▪ 민간 클라우드 검토
공공기관	▪ G-클라우드 ▪ 자체 클라우드	▪ 민간 클라우드 검토	▪ 민간 클라우드 우선

※ 출처 : K-ICT 클라우드 컴퓨팅 활성화 계획, 2015.

- 공공, 금융, 의료 등 주요 사업 분야에서 클라우드 활성화 정책과 충돌하는 규제가 여전히 존재하며 관련 규제 개선을 추진 중

<표 c> 클라우드 컴퓨팅 규제개선 추진 현황

분야	규제명	법령	규제내용	비교
금융 (금융위)	전자금융업 감독일반	정보처리위탁규정	'금융회사의 정보처리 및 전산설비위탁에 관한규정'은 정보처리의 제3자 위탁을 제한, 가능하도록 개선(2015.7월)	완료
교육 (경찰청)	운전학원 등 등록	도로교통법(제101조, 제104호) 및 시행령(별표5)	'운전학원 학사관리 전산시스템 표준규격고시'는 학원내에 서버컴퓨터 등을 갖추도록 하고 있었으나 중앙집중식 서버이용이 가능하도록 개선(2015.5월)	완료
의료 (복지부)	전자 의무기록	의료법(제23조) 및 시행규칙(제16조)	'전자의무기록관리 보존을 위한 장비시설'을 병원에 갖추도록 하고 있어(유권해석), 시행규칙개정 중	시행규칙 입법예고
교육 (교육부)	사이버대학 설립인가 기준 및 절차	평생교육법, 사이버대학설립 ·운영규정(원격교육설비기준고시)	'원격교육설비기준고시'는 서버설비기준 등에서 '물리적으로 별도의 서버를 구성' 하여야 한다고 규정	개정진행
금융 (금융위)	전자금융업 감독일반	전자금융감독규정(제15조) 및 시행세칙(제2조의2)	시행세칙신설에도 불구하고 국내소재전산센터 및 정보처리 시스템은 물리적 망분리를 요구 (시행세칙 제2조의2 제2항)하여 규제 잔존	개정진행
보건·의료 (복지부)	기탁등록 보존기관 지정	생명연구자원의 확보·관리 및 활용에 관한법률(제8조) 및 시행령(제3조)	기탁등록 보전기관 지정요건: 생명연구 자원정보시스템 운영을 위한 전산장비, 백업시설 및 보안시설을 보유하고 이를 관리할 수 있는 전산담당자를 1명이상 확보	검토중
ICT일반 (미래부)	공인전자문서 센터의 지정	전자문서 및 전자 거래기본법 (제31조의2) 및 시행령 (제15조의4) (공인전자문서센터 시설 및 장비 등에 관한 규정)	네트워크 보안기능을 구현하기 위하여 물리적으로 분리된 둘 이상의 네트워크 회선을 갖추고, 시스템을 안전하게 운영하기 위하여 시스템 운영실을 별도의 통제구역으로 구획	검토중
	공인전자문서 중계자의 지정	전자문서 및 전자 거래기본법 (제31조의2) 및 시행령(제15조의14) (공인전자문서중계자인력 ·기술능력, 시설·장비규정)	시설·장비 및 정보를 안전하게 운용하기 위한 보호설비로서 물리적으로 분리된 둘 이상의 망 회선 요구하고, 중계자의 시설 및 장비를 위한 공간은 물리적으로 출입통제가 가능한 별도의 통제구역으로 구획	검토중
주택 (국토부/ 미래부)	초고속 정보통신 건물인증	지능형 홈 네트워크 설치 및 기술기준(제13조)	아파트단지가 '초고속 정보통신 건물'로 인증받기 위해서는 관련 규정에 따라, 반드시 단지 내에 서버를 설치·관리	검토중

※출처 : 관계부처합동, K-ICT 클라우드컴퓨팅 활성화 계획(안), 2015. 재정리.

[참고문헌]

1. 국내문헌

[1] MicroSoft, “클라우드 보안 준수”, 2017.

[2] 정보통신산업진흥센터, “클라우드 서비스 보안기술 동향 - CASB”, 2017.

[3] boannews, “클라우드 보안 솔루션 발표”, 2017.

[4] The Science Times, “해커들이 클라우드 노리는 이유”, 2017.

[5] Slideshare, “클라우드 보안 이슈 및 과제 기반 대응 방안”, 2017.

[6] 테크엠, “동상이몽이 쌓은 벽, 클라우드 확산 막아”, 2017.

[7] LG CNS, “클라우드 컴퓨팅 보안을 위한 정보보호 고려사항”, 2017

[8] 이민화, “4차산업혁명과 규제개혁”강연, 2017.06.

[9] 디지털타임스, “2020년 시장 481조 ‘폭풍성장’클라우드 미래 먹거리 창고 열린다.” 2017.03.

[10] 통계청, “중소기업정보화수준조사 : 클라우드 서비스 이용 여부”, 2016.

[11] IDC, “전세계 퍼블릭 클라우드 서비스 시장 2020년 1,950억 달러 전망”, 2016.

[12] Sciencetimes, “클라우드가 보안에 취약한 이유”, 2016.

[13] 매튜포트노이, “Virtualization Essentials”, 에이콘출판사, 2016.

[14] 한국산업기술평가관리원, “국내외 전기자동차 시장, 기술 및 정책동향”, 2016.

[15] SK C&C, “국내외 클라우드 시장현황”, 2016.

[16] MicroSoft, “액티브 디렉토리”, 2016.

[17] 뉴딜코리아, “클라우드 서비스 보안 취약점 점검”, 2016.

[18] 정보통신산업진흥원, “국내외 클라우드 정책 및 산업동향”, 2016.

[19] 한국정보산업연합회, “클라우드 활성화를 위한 새로운 시각”, 2016.

[20] The Software Alliance, ‘2016 BSA 글로벌 클라우드 컴퓨팅 평가지수’,

2016.

[21] Ddaily,“보안서비스 봇물...‘ SEcaaS’ 시대 막 올랐다”, 2016.

[22] DT, ‘중국 보험사, 클라우드 보험상품 출시’, 2016.

[23] SECURITYWEEK, ‘공공 클라우드 보안에 대해 여전히 염려되는 IT 전문가’, 2015.

[24] MicroSoft, ‘클라우드 환경에서 보안의 중요성’, 2015.

[25] Kossa, ‘클라우드 보안 인증’, 2015.

[26] 이영훈, 기업혁신을 위한 클라우드 여행

[27] 한국인터넷진흥원, ‘클라우드 환경에서의 하이퍼바이저 가상화 기반 보안 기술 동향’, 2014.

[28] 한국인터넷진흥원, ‘클라우드 환경에서의 가상 네트워크 침입방지 및 보안 관리’, 2014.

[29] ZDNetKorea, ‘가상화 보안위협, 클라우드 아킬레스건되나’, 2014.

[30] 보안공학연구논문지, ‘클라우드 보안 위협요소와 기술 동향 분석’, 2013.

[31] 한국클라우드보안협회&CSA, CSA Summit Korea 2013, 2013.

[32] 한국인터넷진흥원, ‘Hypervisor-based Security for Cloud Computing Environments’, 2012.

[33] SKT, ‘올레kt 등의 클라우드보안’, 2012.

[34] 디지털타임스, “삼성화재-SK텔레콤 ‘e-biz 배상책임보험’ 계약 체결”, 2012.

[35] Itworld, ‘KT 유클라우드 비즈, 국제정보보호 인증 획득’, 2012.

[36] 아시아경제, ‘LG U+,아이시어스, 유통,물류 고객정보 보안 위해 맞손’, 2011.

[37] 방송통신진흥원, ‘클라우드 서비스 활성화를 위한 정책 방향’, 2009.

[38] 손해보험사, ‘웜바이러스 피해보상 10억 추정’, 2003.

2. 국외문헌

[1] Infoworld, “The dirty dozen: 12 cloud security threats”, 2016.

[2] Holger Schulze, “Cloud Security : 2016 spotlight report”, 2016.

[3] IMPERVA INCAPSULA, ‘Top 10 Security Concerns for Cloud-Based Services’, 2015.

[4] HJ Lee, Security Consieration for use of Secure Cloud Services, CloudSec 2012,

[5] Hawking, Stephen, and Michael Jackson. A brief history of time. Dove Audio, 1993.

주 의

1. 이 보고서는 소프트웨어정책연구소에서 수행한 연구보고서입니다.
2. 이 보고서의 내용을 발표할 때에는 반드시 소프트웨어정책연구소에서 수행한 연구결과임을 밝혀야 합니다.