클라우드 하이퍼바이저 ESXi 보안 취약점 진단 기준에 관한 연구

김선집[1*], 허진[2]
[1]한세대학원 IT학부 교수, [2]한세대학교 ICT환경공학과 대학원생

A Study On The Cloud Hypervisor ESXi Security Vulnerability Analysis Standard

Sun-Jib Kim[1*], Jin Heo[2]
[1]Professor, Division of Information Technology, Hansei University
[2]Graduate Student, Dept. of ICT Environmental Engineering, Hansei University

요 약 클라우드 컴퓨팅 산업은 ICT 산업의 핵심 요소로써 미래 ICT 산업 발전의 분수령이 될 중요한 산업분야로 평가받고 있다. 우리나라는 제1~2차 클라우드컴퓨팅 발전 기본계획을 수립하여 클라우드 산업의 성장을 유도하고 있다. 하지만 국내 정보보안 가이드에서 Unix 및 Windows 서버, DBMS, 네트워크 장비, 보안 장비의 기술적 취약점 진단 기준은 제시하고 있으나 클라우드 컴퓨팅의 핵심 요소인 하이퍼바이저에 대한 취약점 진단 기준은 제시하지 못하고 있다. 클라우드 시스템을 구축한 기관에서는 본 논문에서 제시한 기준을 활용하여 취약점 진단을 하는데 도움을 받을 수 있을 것이다.

주제어 : 클라우드, 하이퍼바이저, ESXi

Abstract The cloud computing industry is regarded as a key element of the ICT industry and an important industry that will be a watershed for the future development of ICT industry. Korea has established the 1st~2nd cloud computing development basic plan to induce the growth of the cloud industry. However, the domestic information security guide provides technical vulnerability analysis criteria for Unix and Windows servers, DBMS, network equipment, and security equipment, but fails to provide vulnerability analysis criteria for hypervisors that are key elements of cloud computing. Organizations that have deployed cloud systems will be able to assist in vulnerability analysis using the criteria presented in this paper.

Key Words : Cloud, Hypervisor, ESXi

1. 서론

IDC 또는 전산실의 물리적 공간 제약으로 인하여 기존의 온프레미스 환경에서는 인프라를 확장하는데 한계가 존재했다. 이에 하이퍼바이저를 이용한 클라우드 컴퓨팅 시스템의 도입이 조금씩 확산되고 있다.

금융권 기업들은 “전자금융기반시설의 취약점 분석・평가” 기준을 활용하여 정보보안 컴플라이언스에 대응하고 있으며, 그 외 일반 민간 기업과 공공 기관들은 “주요정보통신기반시설 취약점 분석・평가” 기준을 활용하여

*교신저자 : 김선집(kimsj@hansei.ac.kr)
접수일 2020년 7월 20일 수정일 2020년 8월 27일 심사완료일 2020년 9월 14일

정보보안 컴플라이언스에 대응하고 있다.

하지만 이 기준들은 Unix 및 Linux 서버, Windows 서버, DBMS와 같은 전통적인 시스템 취약점 진단 기준만을 제시하고 있으며, 클라우드 컴퓨팅의 핵심 요소인 하이퍼바이저에 대한 취약점 진단 기준은 제시하고 있지 못하고 있다. 따라서 본 논문에서는 시장 점유율이 높으며, 일부 버전은 무료로 제공하여 현장에서 유용하게 사용되고 있는 VMware ESXi의 취약점 진단 기준을 도출하고자 한다.

2. 관련연구

2.1 클라우드 컴퓨팅

클라우드 컴퓨팅이란 인터넷을 이용하여 가상화된 정보 기술(Information Technology) 자원을 언제 어디서나 필요한 만큼 활용할 수 있도록 하는 컴퓨팅 방식이다. 가상화된 IT 자원(CPU, Network, 스토리지 등)을 필요한 만큼 임대해 주고, 자원의 이용률에 따라서 실시간 확장성을 보장하며, 이용한 만큼의 비용을 지불받는 서비스를 클라우드 컴퓨팅 서비스라고 한다[1].

클라우드 컴퓨팅 산업은 ICT 산업의 핵심 요소로써 미래 ICT 산업 발전의 분수령이 될 중요한 산업분야로 평가받고 있다.

클라우드 컴퓨팅은 〈Table 1〉과 같이 클라우드 컴퓨팅 서비스 유형에 따라 응용 소프트웨어를 서비스로 제공하는 SaaS(Software as a Service), 소프트웨어 개발 환경 플랫폼 서비스를 제공하는 PaaS(Platform as a Service), IT 인프라 서비스를 제공하는 IaaS (Infrastructure as a Service)로 분류할 수 있으며, 운영 형태에 따라 기관 내부적으로 구축하여 이용하는 프라이빗(Private) 클라우드, 외부 사업자의 서비스를 활용하는 퍼블릭(Pulic) 클라우드, 프라이빗과 퍼블릭을 조합한 하이브리드(Hybrid) 클라우드로 분류할 수 있다[2].

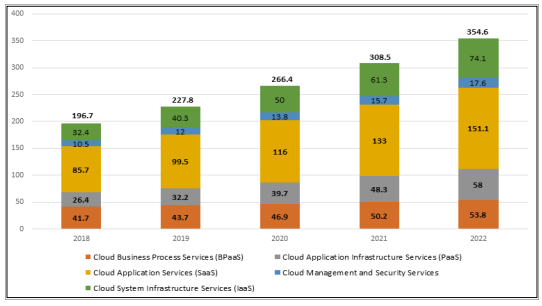
〈Table 1〉 Cloud computing types by Category

Classification		Main Content
Service Type	SaaS	A service that provides software to users
	PaaS	Services that provide users with the platform they need to develop software
	IaaS	Services that provide users with only hardware resources such as CPU, memory, and storage
Operational Type	Private Cloud	A type of providing services only to insiders by establishing a cloud service environment in the internal infrastructure of companies and institutions
	Public Cloud	A type of providing services for unspecified individuals
	Hybrid Cloud	A combination of public and private cloud, providing services by setting private policies for some data and services that do not want to be shared.

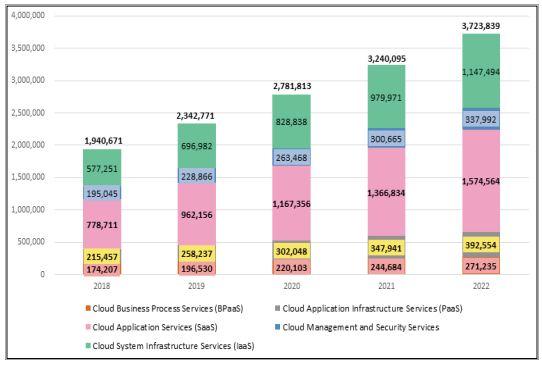
2.2 클라우드 시장 동향

글로벌 IT 자문기관인 가트너는 지난 12월에 2022년 전세계 퍼블릭 클라우드 서비스 시장 규모를 3,546억 달러로 예상하는 시장 전망을 발표했다[3].

[Fig. 1]과 같이 가트너는 클라우드 서비스가 IT기반의 업계의 판도를 바꾸고 있다고 판단하고, 모든 업체들의 비즈니스 모델 및 매출 성장세를 견인할 것이며, 2022년에는 클라우드 서비스 시장 규모 및 성장세가 전체 IT 서비스 성장세의 약 3배에 이를 것으로 분석하여 보고하고 있어 클라우드 시장의 규모가 지속적으로 성장할 것으로 전망하고 있다.



[Fig. 1] Worldwide Public Cloud Service Revenue Forecast (Billions of U.S. Dollars)



[Fig. 2] Korea Public Cloud Service Revenue Forecast

국내 퍼블릭 클라우드 시장 규모 또한 [Fig. 2]와 같이 2019년 2조 3천억원, 2020년 2조 7천억원, 2022년 3초 7천억원으로 연평균 19% 성장할 것으로 전망하고 있다[4].

3. 클라우드 정책 동향

3.1 국외 클라우드 정책 동향

국외에서는 클라우드 관련 산업을 적극적으로 육성하고 국가의 중요한 인프라로 활용하기 위해 다양한 정책들을 내놓고 있다.

미국은 2009년 연방정부의 CIS(Chief Information Officer, 최고정보관리자) 협의회에서 FCCI(Federal Cloud Computing Initiative)을 발표하며 클라우드 컴퓨팅의 이점을 적극 활용하기 시작했다. 2010년에는 연방정부의 IT개선을 위한 25개의 중점과제를 발표하였으며, 클라우드 퍼스트(Cloud First) 정책이 여기에 포함되었다. 클라우드 퍼스트 정책은 정부 기관들이 클라우드 컴퓨팅을 선제적으로 도입할 것을 명시했다. 이에 따라 각 정부부처 및 기관들에는 이를 위한 예산이 편성되었고, 안전성이 보장되며 비용절감이 되는 경우에는 반드시 클라우드 기반의 솔루션을 활용하도록 했다. 클라우드 퍼스트 정책은 2011년 백악관에서 낙후된 IT환경 개선을 위해 '연방정부 클라우드 컴퓨팅 전략'을 발표하면서 실현되었다. 이 발표 이후 NIST(National Institute for Standards and Technology)는 'NIST 클라우드 컴퓨팅 기준 로드맵'을 발표하여 미국의 범정부 클라우드 서비스를 위한 기준과 분류체계를 제시했다[5].

2017년 미국 트럼프 대통령은 'Cloud Only' 행정 명령을 통해 모든 정보화 시스템의 클라우드 전환을 의무화 하도록 했다[5].

영국은 2009년 Digital Britain이라는 차세대 ICT 정책을 내놓으면서 클라우드 산업정책 육성의 일환으로 공공부문 클라우드 도입의 필요성을 제기했다. 2011년에는 좀 더 구체적인 클라우드 도입 전략을 담은 정부 클라우드 전략(Government Cloud Strategy)을 발표했다. 2012년에는 카탈로그 형태로 클라우드 서비스를 찾을 수 있는 조달 체계 전문 쇼핑몰인 'G-Cloud Store'를 개설하여 기존에 개별로 이루어지던 IT서비스 개발의 중복성을 해소했다[5].

2013년에는 공공부문의 IT 인프라를 구축할 때 의무적으로 클라우드 도입을 고려하도록 하는 'Cloud First Policy'를 발표했다. 2017년에는 세부 가이드라인을 통해 민간 클라우드를 우선하도록 하는 'Public Cloud First'로 발전시켰다[5].

3.2 국내 클라우드 정책 동향

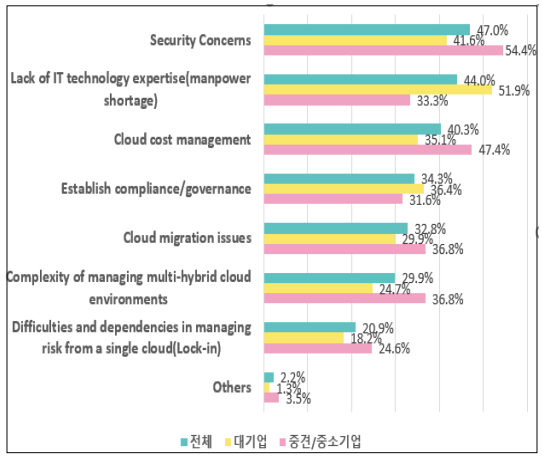
우리나라 정부는 클라우드 산업의 성장을 위해 법·제도적 기반을 마련하며 다양한 정책들을 펼치고 있다. 2009년에는 범정부 클라우드 컴퓨팅 활성화 종합계획을 수립하였으며, 2015년에는 세계 최초로 '클라우드 컴퓨팅 발전 및 이용자 보호에 관한 법률(이하 클라우드발전법)'을 제정하였다.

2015년에는 'K-ICT 클라우드컴퓨팅 활성화 계획(제1차 클라우드컴퓨팅 발전 기본계획)'을 수립하였다. 2018년에는 4차 산업혁명 체감을 위한 클라우드 컴퓨팅 실행(ACT) 전략(제2차 클라우드 컴퓨팅 발전 기본계획)을 수립하였다[6].

4. 클라우드 기반에서의 정보보호 기법

4.1 클라우드 도입 시 우려 사항

국내 기업의 클라우드 도입 속도가 빠르게 증가하고 있다. 이에 [Fig. 3]은 클라우드를 도입 시 여러 가지 우려 사항에 대한 내용으로 그 중에서도 보안에 대한 우려가 47.0%를 차지하며 클라우드 도입 시 겪는 가장 큰 어려움으로 나타났다[7].



[Fig. 3] Concerns when Introducing Cloud Service

또한 미국의 보안 업체 'FireMon'에 따르면 클라우드 서비스 도입 속도가 적시에 해당 서비스를 보호할 수 있는 능력을 넘어섰다는데 동의하는 비중이 60%에 달해 클라우드 보안에 대한 우려가 높은 것으로 나타났다[8].

한편 트렌드마이크로의 '클라우드 보안 위협(Untangling the Web of Cloud Security Threats)' 보고서에 따르면 클라우드 서비스의 설정이 잘못되면 데이터 유출과 같은 위험에 노출될 수 있다고 발표하였다[9].

4.2 국내 정보보안 컴플라이언스

「정보통신기반보호법」시행령 제17조에 주요정보통신기반시설로 지정된 때에는 지정 후 6개월 이내 취약점 분석·평가를 실시하여야 하며, 그 이후에는 매년 취약점의 분석·평가를 실시하도록 명시하고 있다.

취약점 분석·평가를 실시할 때에는 미래창조과학부(現 과학기술정보통신부)고시 제2013-37호 "주요정보통신기반시설 취약점 분석·평가 기준"을 준용하여 실시하여야 하며, 여기에는 관리적 분야, 물리적 분야, 기술적 분야로 주요 점검 내용을 분류하도록 하고 있으며, 가용한 자원과 대상 시설을 식별하고 자산의 중요도를 산정하여 해당 시스템에 대한 정밀분석을 실시하도록 하고 있다.

각 분야별 점검항목에 있어서 관리적 분야는 정보보호 정책 수립, 조직 및 인적 보안 절차, 정보보호 인식 및 교육 훈련 실시 등 관리적인 측면을 점검하도록 명시하고 있으며, 물리적 분야는 주요정보통신기반시설 출입자 통제 및 감시 지원설비 설치 유무 등 물리적인 측면을 점검하도록 하고 있다. 또한, 기술적 분야는 Unix 서버, Windows Server, DBMS, 네트워크 장비, 보안 장비 등의 시스템 설정과 관련한 기술적 측면을 점검하도록 하고 있으며 이에 점검항목의 수는 〈Table 2〉와 같다[10].

〈Table 2〉 Major Information and Communication Infrastructure Targets and Items

Classification	H	M	L	Sum
Unix	43	18	12	73
Windows	45	34	3	82
Security Equipment	16	9	1	26
Network Equipment	14	21	3	38
Control System	16	6	0	22
PC	14	5	1	20
DBMS	11	8	5	24

ISMS-P(정보보호관리체계 및 개인정보보호관리체계) 인증기준의 통제항목 2.11.2 취약점 점검 및 조치에서는 정보시스템의 취약점이 노출되어 있는지 확인하기 위해 정기적으로 취약점 점검을 수행하고 발견된 취약점은 신속히 조치하도록 명시하고 있다[11].

또한,「전자금융거래법」제21조의3(전자금융기반시설의 취약점 분석·평가),「전자금융거래법 시행령」제11조의5(전자금융기반시설 취약점 분석·평가의 절차 및 방법 등)에서는 전자금융기반시설에 대한 취약점 분석 평가를 사업연도마다 1회 이상 하여야 한다고 명시하고 있다.

전자금융 기반시설의 취약점 진단 기준은 "전자금융기반시설 보안 취약점 평가기준 (제2020-1호)"을 통해 확인할 수 있다. 기술 분야는 서버, 데이터베이스, 네트워크 장비, 정보보호시스템을 진단하며 그 점검항목의 수는 〈Table 3〉과 같다[12].

〈Table 3〉 E-financial Infrastructure Targets and Items

Classification	Number of Checklist
Server	159
Database	31
Network Equipment	55
Security Equipment	41

4.3 클라우드 정보보안 컴플라이언스

「클라우드컴퓨팅서비스 정보보호에 관한 기준」 제3조 제1항에서 "클라우드컴퓨팅서비스 제공자는 클라우드컴퓨팅서비스의 안전성 및 신뢰성 확보를 위하여 관리적 보호조치를 취하여야 한다."고 규정하고 있으며, [별표 1] 관리적 보호조치 3.1.1 자산 식별에서 "클라우드컴퓨팅서비스에 사용된 정보자산(정보시스템, 정보보호시스템, 정보 등)에 대한 자산분류기준 수립하고 식별된 자산의 목록을 작성하여 관리하여야 한다."고 명시하고 있다. 또한 클라우드서비스 보안운영 명세서에서는 가상인프라 및 가상자원 취약점 점검을 수행하도록 하고 있다[13].

또한, ISO/IEC 20717:2015에서는 Cloud service extended control set인 CLD.9.5.2 Virtual machine hardening에서 "가상 머신을 구성하는 경우, 클라우드 서비스 사용자 및 제공자는 적절한 기술적 조치 및 보안 환경 설정을 확인하여야 한다."고 규정하고 있다[14].

하지만 클라우드 서비스를 제공하기 위한 핵심 구성요소인 하이퍼바이저에 대한 취약점 진단 기준은 제공하고 있지 않아 컴플라이언스 준수를 위해 취약점 진단을 수

행하는 기관 입장에서는 어려움을 겪고 있다.

2017년에 한국인터넷진흥원에서 클라우드 컴퓨팅 도입/운영/실무 보안을 담은 「클라우드 정보보호 안내서」를 발간하였다. Ⅳ. 클라우드 컴퓨팅 보안에서 '가상화 및 서버 보안'을 다루고 있지만 가상 자원의 생명 주기와 관련된 '관리적 측면'의 내용만 있을 뿐 보안 취약점(Common Configuration Enumeration) 점검 기준은 제시하고 있지 못하다[15].

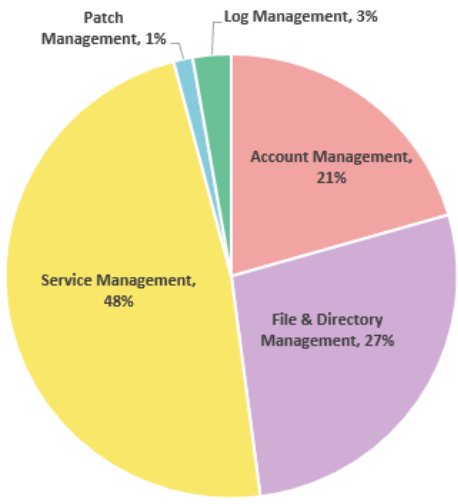
4.4 클라우드 하이퍼바이저(VMware ESXi) 취약점 진단

하이퍼바이저 중에서 VMware는 시장 점유율 41%로 1위를 차지하고 있다[16]. 프라이빗 클라우드(Private Cloud)를 구축하고자 하는 기업에서는 VMware를 이용하는 비율이 높다는 의미이다. 하지만 한국인터넷진흥원에서 배포한 "주요정보통신기반시설 기술적 취약점 분석·평가 방법 상세 가이드" 및 금융보안원에서 배포한 "전자금융기반시설 보안 취약점 평가기준 (제2020-1호)"의 취약점 진단 기준 및 조치 방법은 Unix 또는 Linux에 치우쳐 있으며, 해당 취약점 진단 항목 기준 및 보안 조치 방법은 베어메탈(BareMetal) 유형의 VMwre ESXi에 적용할 수 없다.

〈Table 4〉 및 [Fig. 4]와 같이 "주요정보통신기반시설 기술적 취약점 분석·평가 방법 상세 가이드"의 Unix 서버 진단 영역 중 27%를 차지하는 '파일 및 디렉터리 관리' 영역을 살펴보면 특정 파일 또는 디렉터리의 접근 권한을 변경하도록 권고하고 있다.

〈Table 4〉 Main Information and Communication Infrastructure Diagnosis Areas's Ratio

Classification	Number	Ratio
Account Management	15	21%
File&Directory Management	20	27%
Service Management	35	48%
Patch Management	1	1%
Log Management	2	3%
Sum	**73**	**100%**



[Fig. 4] Main Information and Communication Infrastructure Diagnosis Areas's Ratio

하지만 VMware ESXi는 파일 접근 권한 변경이 불가능하다. VMware ESXi의 /etc/passwd 파일의 접근 권한 기본 설정을 확인해 보면 'rw-r--r-T'임을 확인할 수 있다.

```
[root@192:~] ls -l /etc/passwd
-rw-r--r-T    1 root     root     257 Aug  5  2019 /etc/passwd
```

[Fig. 5] /etc/passwd File access rights

이는 /etc/passwd 파일의 소유자는 읽기 및 쓰기 권한을 가지며, 소유그룹은 읽기 권한, 기타 사용자는 읽기 권한만 가진다는 의미이며, 이 파일은 Sticky bit가 설정되어 있다는 의미이다.

/etc/passwd 파일의 접근 권한을 'rwxrwxrwx'변경해 보았다.

```
[root@192:~] chmod 777 /etc/passwd
[root@192:~] ls -l /etc/passwd
-rwxrwxrwx    1 root     root     257 Aug  5  2019 /etc/passwd
```

[Fig. 6] Change access rights of /etc/passwd File

/etc/passwd 파일의 접근 권한을 변경한 후에 VMware ESXi 시스템을 재부팅 하였다.

[Fig. 7] VMware ESXi Reboot

재부팅이 완료되고 나서 VMware ESXi에 SSH로 접속한 후에 /etc/passwd 파일의 접근 권한을 확인해보면 'rw-r—r-T'로 원상복구 되어 있음을 확인할 수 있었다.

```
[root@192:~] ls -l /etc/passwd
-rw-r--r-T    1 root     root           257 Aug  5  2019 /etc/passwd
```

[Fig. 8] Access to /etc/passwd File After Reboot

이렇듯 기존에 국내 배포된 가이드로는 VMware ESXi의 취약점 진단을 진행할 수 없다. 이에 본 논문에서는 VMware ESXi의 특성 및 기능을 확인하고 VMware ESXi 보안백서의 내용 분석 및 국립표준기술연구원(NIST) 800-53 'Security and Privacy Controls for Information Systems and Organizations'을 통하여 실제 운영 중인 ESXi 호스트에 적용 가능한 보안 취약점 진단 기준을 〈Table 5〉와 같이 도출하였다.

비밀번호가 도용될 수 있는 취약점을 도출하여 '계정관리' 영역으로 구분하였으며, 접근 통제 설정 미흡으로 비인가자의 접근을 허용할 수 있는 설정들은 '접근 제어' 영역으로 구분하였고 VMware ESXi 호스트에 대한 정보를 얻는 방법으로 사용되어 2차 공격을 유발할 수 있는 설정들은 '보안 설정 관리' 영역으로 구분하였으며 마지막으로 보안 패치 적용 여부와 사고 발생 시 감사 추적을 위한 로그 설정 항목들을 도출하여 '패치 및 로그관리' 영역으로 구분하였다.

〈Table 5〉 VMware ESXi Vulnerability Diagnosis items

Check List
1. Account Management
1.1 Set the administrator account as a non-root account
1.2 Set password complexity
1.3 The prohibit the reuse of passwords within five iterations
2. Access Control
2.1 Use a dedicated account other than root when connecting to the Web Console
2.2 Set Account Locking Threshold
2.3 Restrict ssh connection to root account
2.4 Firewall default policy set to Drop
3. Securtiy Settings Management
3.1 Set the ESXi Shell idle timeout
3.2 Set the DCUI idle timeout
3.3 Set the Web Console idle timeout
3.4 Disabled of Managed Object Browser(MOB)
3.5 Set SNMP Community String Complexity
3.6 Set Virtual Switch to Deny Forged Transfer
3.7 Set to deny virtual switch MAC address changes
3.8 Set Virtual Switch Promiscuous Mode to Reject
3.9 Configure NTP time synchronization
4. Patch and Log Management
4.1 Setting Up a Remote Logging Server for an ESXi Host
4.2 Audit Record Settings
4.3 Enable kernel core dump
4.4 Persistent saving of locally stored logs
4.5 Limit VM Log File Size
4.6 Security patches and updates

5. 결론

"주요정보통신기반시설 취약점 분석·평가 기준" 과 "전자금융기반시설 취약점 분석·평가 기준"에서는 운영체제(OS)별 취약점 진단 기준 및 조치 방법을 제시하고 있지만 전세계적으로 이슈화 되고 있는 클라우드 시스템의 기본이 될 수 있는 VMware ESXi와 같은 하이퍼바이저 특성과 맞지 않아 해당 기준으로는 클라우드 시스템의 핵심인 하이퍼바이저에 대한 진단이 어려운 현실이다. 이에 본 논문에서 하이퍼바이저 중에서 시장 정유율이 높은 VMware ESXi의 취약점 지단 기준을 제시하였다.

"주요정보통신기반시설 취약점 분석·평가 기준" 및 "전자금융기반시설 취약점 분석·평가 기준"에서는 Unix 및 Linux의 취약점 조치를 위해 CLI 명령어를 이용하여야 하지만, VMware ESXi에서는 웹 콘솔에서 대부분의 설정 변경작업을 진행할 수 있다. 또한 vCLI 명령어를 지원하여 'esxcli' 및 'vim-cmd '명령어를 이용하여야 하는데 이는 설정마다 지원하는 명령어가 다르기 때문에 명령어마다 지원하는 설정을 잘 파악하여야 한다.

ESXi는 웹 콘솔 웨에도 ESXi Shell, Direct Console

이 있으며, 가상 머신에 네트워크 제공을 위해 Layer 2 기반의 가상 스위치가 존재하므로 이에 대한 보안 진단 기준을 제시하였다.

여기에서 제시된 기준을 바탕으로 진단 방법 및 취약점 조치 방안에 대한 방법이 개발되어 실효성 있는 클라우드 서비스에 대한 취약점 진단을 이행할 수 있도록 지속적인 연구가 진행되어야 할 것으로 판단된다.

REFERENCES

[1] J.Y.Kim, "Self-diagnosis of Suitability for the Introduction of Cloud Services in the Public Sector and a Guidebook for the Introduction of Each," TTA, p.15, 2016.

[2] W.Y.Kang, "Recent Cloud Computing Service Trends," NET Term, p.22, 2013.

[3] Gartner, 2019[Internet], https://www.gartner.com/en/newsroom/press-releases/2019-11-13-gartner-forecasts-worldwide-public-cloud-revenue-to-grow-17-percent-in-2020

[4] Gartner, 2019[Internet], https://biz.chosun.com/site/data/html_dir/2019/04/03/2019040302058.html

[5] S.W.Ahn, "Policy and Direction for Enabling Cloud Computing in Korea," SPRi, pp.1-6, 2019.

[6] M.S.Kang, "Cloud Computing Market Trends and Prospects," KDB Monthly News, Vol.1, No.758, 2019.

[7] "2019 Current State of Domestic Cloud Adoption," Bespin Global, p.19, 2019.

[8] "State of Hybrid Cloud Security," FireMon, p.12, 2019.

[9] "Untangling the Web of Cloud Security Threats," TrendMicro, p.34, 2020.

[10] "Detailed Guide on the Analysis and Evaluation of Vulnerabilities in Major Information and Communication Infrastructure," KISA, p.3, 2017.

[11] "ISMS-P Certification Criteria Guide," KISA, p.175, 2019.

[12] "Guide to Evaluation Criteria for Security Vulnerability of Electronic Financial Infrastructure," FSI p.11, 2020.

[13] "Ministry of Science and ICT public notice 2017-7," MSIT, 2017.

[14] "International Standard ISO/IEC 27017," ISO/IEC p.26, 2015.

[15] "Cloud Security Guide," KISA, p.49, 2017.

[16] ETNews, 2019[Internet], https://m.etnews.com/20190718000155

김 선 집(Sun-Jib Kim) [정회원]

- 2001년 2월 : 숭실대학교 컴퓨터학과 (공학석사)
- 2010년 2월 : 한세대학교 IT학과 (공학박사)
- 2014년 3월 ~ 현재 : 한세대학교 IT학부 ICT 융합학과 교수

〈관심분야〉
정보보안, 사물인터넷, 클라우드, 환경시스템

허 진(Jin Heo) [준회원]

- 2004년 2월 : 단국대학교 과학교육과 (학사)
- 2019년 3월 ~ 현재 : 한세대학교 ICT환경공학과 석사과정
- 2019년 7월 ~ 현재 : ㈜싸이버원 수석컨설턴트

〈관심분야〉
클라우드, 하이퍼바이저, 취약점 진단