

공공 클라우드 기술과 정책의 개선방안에 대한 연구

김소희¹, 이유림¹, 이일구^{2*}

¹성신여자대학교 융합보안공학과 학생, ²성신여자대학교 융합보안공학과 조교수

A Study on the Improvement of Public Cloud Technology and Policy

So Hui Kim¹, Yu Rim Lee¹, Il-Gu Lee^{2*}

¹Student, Dept. of Convergence Security Engineering, Sungshin University

²Professor, Dept. of Convergence Security Engineering, Sungshin University

요 약 코로나19 팬데믹으로 인해 전 세계는 대공황 이후 가장 심각한 위기에 당면하였으며, 언택트 시대라는 새로운 패러다임을 맞이하고 있다. 우리나라도 이에 발맞춰 ‘한국판 뉴딜’을 비롯한 다양한 정책과 법제도를 발표하였지만, 정보의 활용과 정보의 보호 사이에서 갈등하고 있다. 본 논문에서는 공공 클라우드의 정책과 법령 및 기술을 분석하여 한계점을 도출하고, 이를 바탕으로 모든 국민이 평등한 정보 접근권을 보장받으며 신뢰할 수 있는 안전한 환경에서 디지털 서비스를 이용할 수 있도록 ‘범국가적 차원의 공공 가상머신 구축’을 차세대 국가 성장 동력 확보를 위한 핵심과제로 도입하는 방안을 제안하였다. 이를 통해 모든 국민이 저가-저사양의 단말만으로 다양한 디지털 신기술 서비스를 이용할 수 있도록 하며, 정보보호 전담센터 구축을 통해 급증하는 보안 위협에 대응하고자 한다. 또한, 국내 클라우드 관련 법제도가 보안의 중요성을 간과한 채 정보의 활용만을 강조하고 있다는 점을 지적하고, 법제도가 나아가야 할 올바른 방향을 제시한다.

주제어 : 디지털 뉴딜, 코로나19, 디지털 소외, 양극화, 공공 가상머신, 보안

Abstract Due to the Covid-19 Pandemic, the world is facing the most serious crisis since the Great Depression, and is facing a new paradigm of the Untact era. Korea has also announced various policies and legal systems, including the ‘Korean version of the New Deal’, but it is conflicting between the use of information and the protection of information. In this paper, we derive thresholds by analyzing policies, statutes and technologies in the public cloud. Based on this, we propose to introduce the "Building a Nationwide Public Virtual Machine" as a key task to secure the next-generation national growth engine so that all citizens can use digital services in a secure and reliable environment with equal access to information. Through this, all citizens can use various digital new technology services only with low-priced and low-specification terminals, and by establishing a dedicated center for information protection, we want to respond to rapidly increasing security threats. It also points out that the domestic cloud-related legal system only emphasizes the use of information while overlooking the importance of security, and suggests the right direction for the legal system to move forward.

Key Words : Digital New Deal, COVID-19, Digital Lag, Polarization, Public virtual machine, Security

*This work was partly supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (No. 2020R1F1A1061107) and Korea Institute for Advancement of Technology (KIAT) grant funded by the Korea Government (MOTIE) (P0008703, The Competency Development Program for Industry Specialist).

*Corresponding Author : Il-Gu Lee(iglee@sungshin.ac.kr)

Received May 23, 2021

Revised June 12, 2021

Accepted August 20, 2021

Published August 28, 2021

1. 서론

4차 산업혁명이 가속화되고 지능정보사회가 도래함에 따라, 전 세계는 정치, 경제, 의료 등 전통적인 산업 분야와 신기술을 융합해 신성장 동력을 경쟁적으로 발굴하고 있다. 이러한 시대적 흐름에 따라, 디지털과 소프트웨어 중심의 인프라가 발전하였으며, 공유 플랫폼을 이용한 디지털 자산의 활용이 급격히 증가하는 추세이다. 그리고 코로나 19의 대유행으로 비대면·온라인이 뉴노멀이 되면서 안전하고 유연한 디지털 자원 활용에 대한 수요도 급증했다.

정부는 코로나 19라는 위기를 IT 최강국으로 도약하기 위한 기회의 발판으로 삼고, 공공 부문의 데이터 활용 활성화를 위하여 각종 정책을 펼치고 있다[1]. 한국판 뉴딜 중 디지털 뉴딜은 빅데이터, 사물인터넷, 블록체인, 5G, 인공지능 등의 기술을 활용해 전 산업 분야의 디지털 전환을 촉진하고자 한다[2]. 디지털 정부혁신 발전계획은 디지털 공공 서비스를 제공하고, 민간 활용도가 높은 공공 데이터 개방을 확대해 각종 디지털 정책의 기반을 다질 것을 계획하고 있다[3].

공공 클라우드란 이러한 디지털 정책의 핵심이 되는 디지털 인프라로, 공공기관의 업무 수행을 위하여 민간 클라우드를 정부 규정 및 지침에 따라 구축한 별도의 클라우드 서비스이다[4]. 가트너에 따르면, 2021년에는 세계 클라우드의 시장 규모가 약 2,783억 달러일 것으로 예상하며, 우리나라 정부는 2025년 이내에 모든 공공기관 업무 수행을 위한 도구를 클라우드로 전환할 것이라고 계획하고 있다[5]. 공공 클라우드 또한 도입 초기에는 사용률이 미비했으나, 최근 관련 지침, 정책, 법령이 제정되면서 이에 대한 관심이 높아지고 있다.

공공 클라우드 기술의 발전으로 정부가 목표를 달성하기 위해서는 디지털 전환 가속화로 발생 가능한 문제점에 얼마나 대응 및 해결 가능한지가 관건일 것이다. 본 논문에서 주목하고 있는 디지털 전환 가속화로 발생 가능한 문제는 다음과 같다.

첫째, 디지털 빈부격차로 인한 양극화 심화이다. 2019년 디지털 정보격차 실태조사에 따르면, 우리나라의 디지털 기술 수준은 준수한 편이지만, 지역·계층 간의 격차가 큰 편이며, 정보취약계층의 디지털 정보화 수준은 69.9%에 그친다[6,7]. 지역·계층 간의 디지털 정보화 수준 차이를 고려하지 않은 채로 디지털 전환이 가속화된다면 정보 격차는 더욱 벌어질 것이다. 디지털 빈부격차의 심화는 디지털 기기 소지 여부에 그치는 것이 아니라, 정보

수집 속도, 정보 수집량, 교육의 기회 등의 면에서 차이를 가져올 수 있으며, 새로운 형태의 불평등을 야기하고 있다[8]. 또한, 새로운 형태의 불평등은 국민에게 정치·경제·사회·문화적 생활의 모든 영역에서 균등한 기회를 보장해줄 것을 명시하고 있는 헌법 제11조 평등권의 침해로 이어질 수 있다.

둘째, 보안 사고의 증가이다. 코로나 19로 재택 근무와 비대면 서비스가 증가함에 따라 온라인 상에서의 데이터 공유량은 늘어나고 있다. 그리고 생체 인증의 활용 범위가 확대되면서, 정보보안은 포스트 코로나 시대의 주요 이슈로 떠올랐다[9]. 그러나 온라인 상에서 거래, 유통되는 디지털 자산은 유출이 쉽고, 약간의 노이즈 추가로 원본과 다른 파일처럼 보이게 하는 등의 발전된 위조 기술로 인해 복제될 위험성이 크다[10]. 그리고 이글루시큐리티의 2021년 보안 위협·기술 전망 보고서에서 발표한 5가지 보안 위협 중 2가지가 코로나 19 이슈에서 파생된 것으로 분석되고 있으며, 포스트 코로나 시대를 겨냥한 사이버 공격이 증가할 것으로 예상된다[11]. 그리고 SK 인포섹 시큐디움(Secudium)에 따르면, 2020년 상반기에 탐지 및 대응한 사이버 공격은 약 310만 건으로, 2019년 상반기에 비해 약 19% 증가했다. 또한, 2020년 국내 기업들의 데이터 침해비용은 2019년 대비 7% 증가한 38억이다[12].

상술한 디지털 양극화와 보안 사고 문제를 개선하기 위한 기술과 정책이 요구된다. 포스트 코로나 시대에 새롭게 등장할 수 있는 불평등과 경제적 불안정성을 해소하기 위해서는 포용적이고 균형적인 디지털 국가 전략을 모색해야 한다[13]. 그리고 데이터의 활용도와 중요도가 높아지는 디지털 전환된 시대에서 IT 최강국으로서의 위상을 유지하기 위해서는 정책과 기술을 보완해 보안 허점을 해결하는 것이 선제적으로 이루어져야 한다[14]. 본 논문은 국내 종래 정책 및 기술의 분석을 통해 디지털 전환으로 야기될 수 있는 문제점 해결에 공공 클라우드의 활용이 적합한가를 평가하고자 한다. 그리고 공공 클라우드로 인한 국가 발전을 이루기 위하여 디지털 자산의 안전한 공유, 거래, 유통을 가능하게 하는 ‘공공 가상머신’ 기술을 설명하고 활용 가치를 높이기 위한 정책을 제안하고자 한다.

본 논문의 구성은 다음과 같다. 2장에서는 공공 클라우드 관련 지침 및 법령을 분석하고, 3장에서는 종래 기술을 분석한다. 4장에서는 정책의 방향성과 개선 방안을 제안하고, 5장에서 결론을 맺는다.

2. 공공클라우드 현황과 관련 지침 및 법령 분석

본 장에서는 공공 클라우드 현황과 공공 클라우드 관련 지침 및 법령을 분석하고, 종래 지침 및 법령의 한계점을 지적하고자 한다. 그리고 이후 이어질 제안하는 정책의 방향의 근거를 제시하고자 한다.

2020 클라우드 산업 실태조사에 따르면, ‘보안’은 클라우드 산업 발전을 위해 필요한 기술과 클라우드 산업의 활성화를 저해하는 요인에서 모두 1순위를 차지했다 [14]. 이처럼 클라우드 산업에서 보안은 매우 중요한 요소이며, 공공 업무를 수행하는 데 사용될 공공 클라우드에 있어서는 더욱 중점적으로 고려해야 할 요소이다. 그러나 데이터와 서비스 활용률을 향상시키기 위해 관련 지침에서는 보안에 대한 규제를 완화하고 있어서 개인정보보호와 프라이버시에 대한 우려가 커지고 있다.

행정·공공기관 민간 클라우드 이용 가이드라인은 행정기관 및 공공 기관에서 민간 클라우드를 공공 클라우드로서 사용함에 있어 안정성, 효율성을 보장하기 위한 지침이다. 이 가이드라인에 따르면, 학교의 교육 목적 이용이나 민간 클라우드 이용협회의 검토를 거친 경우에는 보안 인증이 되지 않은 민간 클라우드를 이용할 수 있다 [15]. 그러나 공교육에 보안 인증이 되지 않은 민간 클라우드가 사용될 경우, 교육자료의 저작권 문제가 발생할 수 있으며, 학생들의 개인정보, 시험 정보 등이 유출되거나 조작되는 등의 사고가 발생할 수 있다. 그러므로 교육용으로 클라우드를 사용하는 경우에도 클라우드의 보안 인증이 필수적이다.

클라우드 서비스 보안인증제 운영 변경 관리서에 따르면, 클라우드 보안 인증제에 대한 유효 기간은 3년에서 5년으로 변경되었다[16]. 이는 2019년 클라우드 보안인증 사업자를 대상으로 진행한 간담회의 논의 결과를 반영한 것으로, 공공기관의 데이터 관리 책임성보다는 클라우드 제공 사업자의 불편을 해소시키는 방향으로 규제가 완화된 것이라 볼 수 있다. 또한, 매년 1회 이상 클라우드에 대해 수행하여야 하는 사후 평가 운영 방식도 완화되었다. 기존 사후 평가는 CCE(Common Configuration Enumeration)점검에 대해 기존 자산의 1/3을 샘플링하고, CVE (Common Vulnerability Exposure) 점검을 최초 평가와 동일하게 진행되었다. 그러나 개선된 사후평가에서는 CCE 점검에 대해 기존 자산의 샘플링 수를 1/3에서 1/4로 줄였으며, CVE 점검은 반기별 사후관리

증적으로 대체하고 사후 평가를 진행하지 않는다.

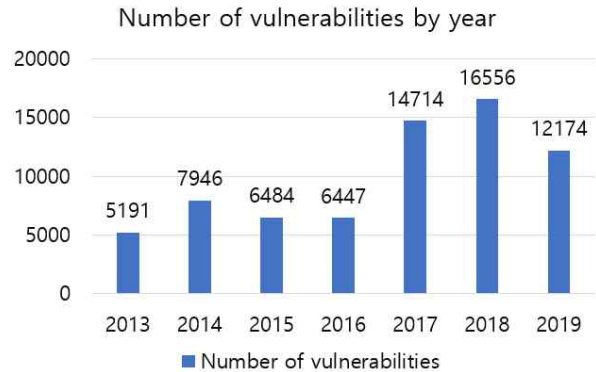


Fig. 1. Number of vulnerabilities by year (CVE Details, 2020)[17]

Fig. 1.은 CVE Details에서 제공한 Vulnerabilities By Year를 재구성한 표로, 연도별 새롭게 발견된 CVE의 개수이다. CVE는 공개적으로 알려져있는 컴퓨터의 보안 결함을 목록화한 것이다. 그림 1에 따르면, 2017년에 새롭게 보고된 CVE는 전년도 대비 두 배 이상 증가하였으며, 2017년 이후에는 매년 무려 10,000건 이상이 꾸준히 보고되고 있다. 그런데 공공 클라우드의 사후 평가 항목 중 CVE 점검을 제외하는 것은 CVE의 증가 추세를 고려하지 않은 규제 완화이며, 이로 인해 취약점 공격에 대한 노출이 증가될 수 있다.

공공 클라우드는 디지털 전환을 도모하기 위한 디지털 뉴딜 등의 정책에 더불어 전자 정부로서의 자리매김과 깊은 관련이 있다. 정부는 2025년 이내에 모든 공공 행정 업무에 공공 클라우드를 도입할 것을 계획 중에 있으며, 공공 서비스 업무는 공공 클라우드 위에서 수행될 것이다. 정보기술을 활용해 ‘전자 정부’로서 신뢰를 얻고 혁신적 포용 국가로 거듭나기 위해서는 사회 서비스 및 공공 서비스를 제공하는 기관의 공적 책무성이 강화되어야 하며, 서비스의 공적 공급이 확대되어야 한다[18]. 그러나 관련 지침 및 정책에서는 디지털 소외계층에 대한 고려가 부족한 실정이다.

디지털 정부혁신 발전계획의 경우, 민원 신청, 생활불편신고 등을 할 수 있는 공공 서비스를 정부가 직접 운영하는 웹-앱에서만 이용할 수 있도록 한다[3]. 이는 신속한 민원 처리를 가능하게 하지만, 디지털 기기를 소지하고 있지 않거나 디지털 기기 활용 능력이 낮은 디지털 소외계층에게는 다소 어려운 민원 처리 방식일 수 있다. 통계청 조사에 따르면, 서비스의 이용이 어렵고 불편하다는

것이 전자정부 서비스의 불만족 원인으로 3위를 차지했다[19]. 그리고 디지털 뉴딜 계획은 전 산업 분야에서 디지털 전환을 활성화하고 국민에게 ICT 융합 서비스를 제공하고자 한다[2]. 그러나 최신 ICT 기기를 활용해 간편하게 건강 관리를 돕고자 하는 건강 취약 계층 및 고령층의 비대면 헬스케어의 목표는 정책 적용 대상 계층이 디지털 활용 능력이 부족하다는 점을 충분히 고려하지 못했다. 그리고 교육 분야에서 이러닝 및 에듀테크 활성화를 도모하고자 하지만, 질 좋은 기기가 없어 온라인 수업 수강이 어려운 학생들에 대한 방안은 제시하고 있지 않다. 디지털 소외계층 학생들에 대한 고려의 부재는 교육의 불균등 문제를 초래할 수 있다.

또한, 통신비 부담 문제를 해결하지 않고 정책, 교육 등의 공공 영역이 온라인으로 확대 및 대체된다면 양극화는 더욱 심화될 것이다. 온라인 서비스를 이용하기 위해서는 인터넷 연결이 필수적이며, 온라인 교육 등 서비스 특성에 따라 장시간 인터넷 연결이 필수적이거나 멀티미디어 콘텐츠를 시청 및 다운로드해야 하는 경우가 있다. 그러나 한국의 무선 데이터 통신비는 OECD 국가 평균 대비 3배 이상이다. 통신비 부담 문제를 해소하기 위하여 월 2만 원에 데이터 1GB, 음성 전화 200분, 문자 메시지를 무제한으로 제공하는 요금제인 보편 요금제를 추진하였으나 통신사와의 이해관계 충돌로 법제화까지는 이어지지 않았다. 이에 국민들은 여전히 공공 서비스를 이용하고 기본권을 보장받기 위하여 무선통신요금을 부담하게 되었다. 국가는 비대면 공공 서비스 확대 이전에 통신사와의 이해관계 충돌을 해소할만한 방안을 포함해 무선통신비 부담을 완화할 방안을 구체적으로 계획 및 시행해야 한다.

공공 클라우드 관련 법령으로는 클라우드 컴퓨팅 발전 및 이용자 보호에 관한 법률, 개인정보보호법, 전자정부법 등이 있다. 그러나 2020년 2월 개정된 개인정보보호법은 전자정부법, 클라우드 컴퓨팅 발전 및 이용자 보호에 관한 법률과 모순되는 조항을 가지고 있으며, 프라이버시 문제로 이어질 수 있는 조항이 추가되었다.

개인정보보호법 제15조 3항은 안전성 확보 조치 여부, 정보주체에게 불이익 발생 여부 등을 고려해 개인정보처리자가 정보주체의 동의 없이 개인정보를 이용할 수 있다고 명시하고 있으며, 제17조 4항은 개인정보처리자의 수집 목적과 합리적으로 관련된 범위에서 제15조 3항의 조건을 고려하여 개인정보처리자가 정보주체의 동의 없이 개인정보를 제공할 수 있다고 명시하고 있다. 그러나 이는 전자정부법 제12조의3(등록시스템의 구축·운

영 등)에서 명시하고 있는 민원인의 사전동의를 받아 다른 행정기관 등이 보유한 자료의 제공을 요청할 수 있다는 조항과 모순된다. 또한, 법원의 제출명령이나 법관이 발부한 영장이 없다면 이용자의 동의 없이 이용자 정보를 제3자에게 제공하거나 서비스 제공 목적 외의 용도로 이용할 수 없음을 명시하고 있는 클라우드 컴퓨팅 발전 및 이용자 보호에 관한 법률 제27조(이용자 정보의 보호)와도 모순된다. 이 모순점에서 국민의 개인정보 및 민감 정보는 유출될 수 있으며, 정보주체는 이로 인한 2차 사이버 공격의 피해를 입을 수 있다.

클라우드 컴퓨팅 발전 및 이용자 보호에 관한 법률의 경우, 정보보호에 관한 규정이 필요성 대비 미약하다. 클라우드 컴퓨팅 발전 및 이용자 보호에 관한 법률 제4장 제23조(신뢰성 향상)에서 명시한 바에 따르면, 클라우드 컴퓨팅 서비스 제공자는 과학기술정보통신부장관이 고시한 정보보호에 관한 기준을 지킬 것을 권고받을 수 있다[20]. 그러나 법령에서 클라우드 컴퓨팅 서비스 제공자에게 정보보호에 관한 기준을 기술적으로 지킬 것을 강제하지 않는다면, 클라우드 컴퓨팅 서비스는 각종 보안 이슈의 피해 대상이 될 것이며, 이 법 조항이 공공 클라우드에도 적용된다면 피해 규모는 보다 확대될 것이다.

3. 공공 클라우드 관련 기술 분석

본 장에서는 기업 중심의 공공 클라우드와 정부 주도 공공 클라우드를 기술적인 관점에서 비교·분석하고, 한계점을 도출한다.

3.1 공공 클라우드 현황

공공 클라우드란 민간 클라우드를 공공기관의 업무에 활용하기 위하여 정부 규정 및 지침에 맞추어 재구축한 클라우드이다. 정부는 공공 업무 수행의 유연성과 효율성 및 보안성을 개선하기 위하여 공공 클라우드를 도입하고 있으며, 최근에는 KT, 네이버 클라우드 플랫폼, NHN TOAST 등 여러 기업에서 공공 클라우드를 제공하고 있다.

공공 클라우드의 활용 방식인 민관 협력형 모델(PPP: Public Private Partnership)은 다음과 같다. 공공기관은 임대 이용료를 지불한 뒤, 내부에 클라우드 서비스 제공 민간 기업의 서버를 설치한다. 공공기관에서는 해당 서버에 시스템을 이관해 인공지능, 블록체인 등의 신기술을 적용하고 업무의 효율성을 제고한다.

공공 클라우드에서 지원하는 서비스는 씨앗(CEART),

NiCloud, PaaS-TA 등이 있다. 씨앗은 클라우드 서비스를 선정하는 데 필요한 정보를 얻을 수 있는 디지털 서비스 마켓 플랫폼이다[21]. 디지털 서비스 이용자와 서비스 제공자는 씨앗에서 정보를 주고받을 수 있다. 이용자는 국가나 공공기관 뿐 아니라, 민간기업 또는 개인이 될 수 있으며, 원하는 서비스를 체험, 신청, 검색, 구매할 수 있다. 서비스 제공자는 소프트웨어, 플랫폼 등을 제공하는 기업으로, 협약, 홍보, 판매, 서비스 제공을 할 수 있다. 그리고 씨앗 플랫폼의 모든 서비스를 무료로 이용할 수 있으며, 유사 서비스를 비교할 수 있다는 장점이 있다. 그러나 클라우드 서비스 검색이 불편하다는 단점이 있다. 씨앗은 클라우드 서비스를 보안, 컴퓨팅, 네트워킹, 스토리지 등의 카테고리 별로 확인할 수 있도록 제공하고 있다. 그러나 카테고리 내에서는 개발 플랫폼 지원, 비즈니스 분석 등의 서비스 내용이 아닌 클라우드 구축 방식, 인증 정보 등으로만 필터 검색을 수행할 수 있다.

NiCloud는 클라우드 기반의 공공 협업 환경이다[22]. 사용자는 NiCloud를 활용해 클라우드를 저장소뿐 아니라 타임라인 소셜 서비스, 웹 오피스, 영상회의 등을 수행할 수 있다. NiCloud의 활용으로 기관 내 협업과 자료 공유를 같은 업무망에서 수행할 수 있으므로 망 이동 시간과 팀별 보고서 취합 등에 소요되는 시간을 줄일 수 있다는 장점이 있다. 그러나 구글 문서와 구글 드라이브 간의 연동 등 유사 서비스가 많이 존재하며, 구글 드라이브의 1인당 최대 무료 용량은 15GB인 반면, NiCloud의 1인당 저장소 용량은 10GB라는 단점이 있다.

PaaS-TA는 클라우드 인프라 환경과 응용 프로그램을 안정적으로 운영 및 제어할 수 있도록 하는 관리 플랫폼이다[23]. PaaS-TA는 오픈 소스 아파치 라이선스로 개발되어 누구나 쉽게 활용 가능하다는 특징이 있다. 그리고 인프라 활용 중심이던 국내 클라우드 산업이 자체적으로 개발한 새로운 개발 및 활용 플랫폼을 바탕으로 상용 서비스를 제공하는 방향으로 변화한다는 의미를 갖는다. 그러나 오픈소스 소프트웨어이므로 더 많은 사용자들이 유입되어야 플랫폼이 발전될 수 있다는 한계점이 있다.

3.2 정부 주도 공공 클라우드

클라우드가 한국판 디지털 뉴딜 사업의 큰 축을 이루게 되면서, 공공 클라우드 시장이 급속도로 활성화되고 있다[24]. 정부에서도 'PaaS-TA'와 같은 클라우드 플랫폼을 개발하는 등 공공 클라우드 발전에 많은 노력을 기울이고 있다.

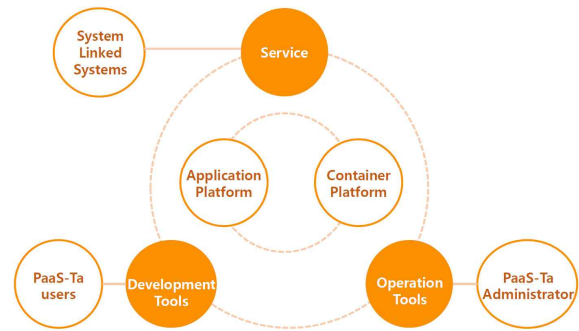


Fig. 2. PaaS-TA Diagram[23]

PaaS-TA는 한국지능정보사회진흥원(NIA)을 중심으로 다양한 국내 업체와의 협업을 통해 만든 정부 주도 공공 클라우드로서 Fig. 2와 같이 애플리케이션/컨테이너 플랫폼, 서비스, 운영도구, 개발도구로 구성되어 있다[23]. 애플리케이션 및 컨테이너 플랫폼은 애플리케이션의 개발 및 배포, 실행/운영 관리를 위한 서비스를 제공한다. 또한, 서비스는 응용애플리케이션 실행 시 다양한 대외 백엔드 플랫폼과 서비스의 연계를 위한 브로커 역할을 수행하며, API(Application Programming Interface) 관리 서비스를 제공한다. 운영도구는 인프라 제어 및 연동과 애플리케이션 플랫폼 관리 서비스를 제공하며, 개발도구는 응용애플리케이션을 개발, 배포, 운영하기 위한 셀프서비스 포털과 개발도구를 제공한다.

PaaS-TA는 전자정부 표준 프레임워크가 탑재되어 있어 공공 부문 적용이 원활하다는 장점이 있다. 비용적인 측면에서는 Cloudfoundry 기반의 오픈소스로 이루어져 있어 이용료가 부과되지 않으며, 기술 지원 역시 별도의 비용 청구 없이 이루어진다. 그러나 PaaS-TA를 활용하기 위해서는 수십여 개의 컴포넌트에 대해 이해하고 있어야 하며, 상대적으로 무거운 클라우드 파운드리 기술에 기반하고 있고, 수많은 오픈소스가 복합되어 호환이 어렵다는 한계를 지니고 있다.

3.3 기업 중심 공공 클라우드

클라우드가 한국판 디지털 뉴딜 사업의 핵심 인프라로 자리 잡으면서 공공 클라우드에 대한 기업들의 관심도 뜨겁다. 특히 2021년 공공 클라우드 분야의 사업 규모가 약 1조원을 넘을 것으로 전망되면서 공공 클라우드 시장이 더욱 활성화되고 있다.

공공 클라우드 서비스를 제공하고 있는 대표적인 기업은 KT이다. KT는 대한민국 정부 및 공공기관 전용 KT G-Cloud 서비스를 제공하고 있다. KT G-Cloud 서비

스는 내부가 DMZ(Demilitarized zone)와 Private zone으로 분리되어 있어 중요한 정보를 폐쇄된 Private zone에 안전하게 보관할 수 있다는 특징이 있다. Private zone은 전용 회선 혹은 VPN(Virtual Private Network)을 통해서만 접근 가능하다. 또한 하드웨어 기반의 침입탐지 시스템과 방화벽을 기본으로 제공하여 높은 안전성을 보장한다. 그러나 이윤을 추구해야 하는 기업의 특성상 정부 주도 공공 클라우드에 비해 상대적으로 고가라는 단점이 있다. 또한 국내 클라우드는 해외에 비해 상대적으로 낮은 기술 수준을 보유하고 있으며, 전문 인력이 부족하다는 한계를 지니고 있다[25].

Table 1. Government and Enterprise Cloud Comparison

Features	Government (PaaS-TA)	Enterprise (KT G-cloud)
IaaS (Infrastructure as a Service)		V
PaaS (Platform as a Service)	V	V
DaaS (Desktop as a Service)		V
Fee High		V
E-government framework support	V	

Table 1.은 정부주도 공공 클라우드와 기업 중심 공공 클라우드를 비교한 표이다. 정부주도 공공 클라우드는 PaaS-TA를 중심으로, 기업주도 공공 클라우드는 KT G-Cloud를 중심으로 비교하였다. 정부주도 공공 클라우드는 대부분 전자정부 표준 프레임워크가 탑재되어 있어 정부 및 공공기관에 적용하기 적합하고 가격이 저렴하다는 장점이 있지만, 다양한 클라우드 서비스를 제공하지 않는다. 예컨대 PaaS-TA의 경우 PaaS만을 제공하고 있다. 반면에 기업 중심 공공 클라우드는 다양한 클라우드 서비스를 제공하고 있다. KT G-Cloud의 경우 IaaS와 DaaS를 제공하며, 정부의 지원을 받아 PaaS-TA 서비스까지 탑재하였다. 하지만 상대적으로 고가이며, 전자정부 프레임워크가 탑재되어 있지 않아 전자정부 서비스로의 도입이 상대적으로 어렵다.

최근 기업 주도의 공공 클라우드는 운영비가 사업 수익 보다 큰 구조적 문제 때문에 B2C보다 B2B 클라우드 사업 중심으로 발전하고 있다. 이러한 추세는 디지털 정보격차를 해소하고 모든 국민이 평등한 정보접근권을 가지도록 하는 데 기여하기 어렵다. 이를 개선하기 위해 본 논문에서는 사회 기반 시설로서 모든 국민이 저렴한 가격으로 다양한 디지털 신기술을 이용할 수 있는 공공 가

상머신 개념과 제도를 제안한다.

4. 개선 방안

한국판 뉴딜 정책에서 클라우드가 큰 축을 이루게 되면서 공공 클라우드 시장이 급격히 활성화되고 있다. 하지만 앞서 살펴보았듯, 디지털 전환의 가속화로 인해 디지털 빈부격차가 심화되고 있고, 보안 위협이 급증하고 있다. 또한, 국내 클라우드 관련 지침은 공공 클라우드의 필수 요소인 보안의 중요성을 간과한 채 보안 규제를 완화하는 방향으로의 전환을 추진하고 있다.

4.1 공공 클라우드 기술

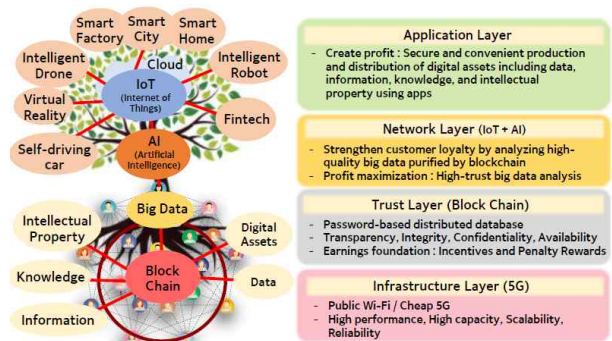


Fig. 3. Public Virtual Machines Concept

Fig. 3.은 본 논문에서 제안하는 공공 클라우드인 ‘공공 가상머신’의 개념도이다. 공공 가상머신은 복수 개의 클라우드가 네트워크로 연결된 대규모 클라우드를 이용해 다양한 애플리케이션과 서비스를 제공하는 디지털 생태계다. 공공 가상머신은 Fig. 3.과 같이 인프라 계층, 신뢰 계층, 네트워크 계층, 애플리케이션 계층으로 이루어져 있다. 사용자는 공공 가상머신에 접속하여 고성능의 인프라를 무료로 이용할 수 있으며, 이를 기반으로 다양한 애플리케이션을 사용할 수 있다. 공공 가상머신에서 생성된 빅데이터는 스마트 네트워크를 통해 분석되며, 암호기반 분산 데이터베이스에 축적된다.

사용자는 네트워크에서 IaaS, SaaS, PaaS 클라우드를 선택하여 사용할 수 있다. 즉, 사용자는 공공 가상머신에 접속할 때마다 원하는 클라우드 서비스를 선택할 수 있고, 이후 해당 서비스를 즉시 가상머신의 형태로 제공 받게 된다. 예컨대 사용자가 IaaS를 선택하면 컴퓨팅 자원을 가상화하여 가상머신으로 제공한다. 사용자의 단말은 입출력 및 네트워킹 역할만을 수행하며 정보의 분석·

처리·가공·저장은 대규모 클라우드 데이터센터에서 수행된다. 따라서 인터넷이 가능한 환경이라면 저가·저사양의 단말만으로도 모든 서비스를 이용할 수 있다. 한 예로 저가·저사양의 단말을 보유하고 있더라도, 공공 가상머신을 활용하면 고사양의 노드가 요구되는 신기술 실습 교육에 참여할 수 있다. 이처럼 사용자는 공공 가상머신에 접속하여 필요한 애플리케이션과 인프라를 이용해 데이터와 서비스를 이용할 수 있다. 또한, 공공 가상머신은 정보보호 전담기관에 의해 보안 관리가 이루어지기 때문에 데이터와 소프트웨어가 통제 가능한 환경에 놓이게 되어 불법 복제 및 데이터 유출 방지가 용이하고, 보안에 취약한 개인 컴퓨팅 환경 대비 안전한 환경을 제공한다.

4.2 종래 기술과 공공 가상머신 비교

종래 공공 클라우드는 공공기관만을 대상으로 클라우드 서비스를 제공하고 있지만, 공공 가상머신은 범국가적 차원에서 대규모 클라우드를 구축하여 공공기관, 국민, 기업 모두에게 인프라와 애플리케이션을 제공하는 형태이다. 또한, 종래 공공 클라우드는 서비스 제공자에게만 컴퓨팅 자원을 제공하여 서비스를 이용하는 개인은 서비스 이용에 필요한 사양의 노드를 갖추어야 하지만, 공공 가상머신 기반의 서비스는 서비스 이용자에게도 컴퓨팅 자원을 제공하여 인터넷이 가능한 환경에 위치하면 저가·저사양의 단말만으로도 모든 서비스를 이용할 수 있다. 이를 통해 국가는 디지털 빈부격차를 완화할 수 있으며, 전자정부 서비스의 활성화를 도모할 수 있다. 또한, 공공 가상머신에 접속할 때마다 원하는 클라우드 서비스(IaaS, PaaS, SaaS 등)를 선택하여 가상머신으로 제공할 수 있어서 사용자는 필요에 따라 즉시 다양한 클라우드 서비스를 이용할 수 있다.

4.3 정책 개선 방안

4.3.1 법적 규제 절충안 마련

정보의 활용과 정보의 보호는 동전의 양면과 같은 존재이다. 공공 클라우드 시장 활성화를 위해서는 법적 규제를 완화하는 것이 바람직하지만, 공공기관은 많은 중요 정보를 다루고 있는 만큼 보안과 관련된 법적 규제를 강화할 필요가 있다.

우리나라는 4차 산업혁명 시대에 발맞춰 정보의 활용을 강화하기 위해 데이터 3법 개정안을 발표했다. 개인정보보호법 제15조 제3항과 제17조 제4항에서는 개인정보 처리자는 당초 수집 목적과 합리적으로 관련된 범위에서

정보주체에게 불이익이 발생하는지 여부, 암호화 등 안전성 확보에 필요한 조치를 하였는지 여부 등을 고려하여 대통령령으로 정하는 바에 따라 정보주체의 동의 없이 개인정보를 이용 및 제공할 수 있다는 조항을 신설했다. 그리고 동법 제28조의2 제1항에서는 개인정보처리자는 통계작성, 과학적 연구, 공익적 기록보존 등을 위하여 정보주체의 동의 없이 가명정보를 처리할 수 있다는 조항을 신설했다. 여기서 통계작성이라 함은 시장조사와 같은 상업적 목적의 통계 처리도 포함하고 있다[26]. 데이터 3법 개정안에는 ‘가명정보’라는 새로운 개념이 도입되었는데, 가명정보는 여러 정보들을 결합하면 특정 개인이 식별될 수 있는 문제점을 안고 있다. 이로 인해 인권침해를 우려하는 목소리도 큰 상황이다. 이처럼 데이터 3법은 정보 활용의 측면에서는 더욱 발전된 입법이었지만, 정보보호의 측면에서는 위험의 증가가 불가피한 결정이었다.

그 뿐만 아니라 클라우드 서비스 보안 인증제 역시 규제가 완화되는 방향으로 변경되었다. 클라우드 서비스 보안 인증제 운영 변경 관리서에 따르면 클라우드 보안 인증제의 유효기간은 더욱 증가하였으며, CCE 점검의 경우 기존 자산의 샘플링 수를 1/3에서 1/4로 줄였고, 사후 평가 항목에서는 CVE 점검을 제외하였다. 이는 사업자의 불편함을 해소함으로써 클라우드 시장의 활성화는 기대할 수 있으나, 보안은 더욱 약화시키는 결정이었다.

우리는 언택트 시대를 살아가면서 국민의 개인정보를 안전하게 보호하는 동시에 디지털 사회로의 전환이 활발히 이루어질 수 있도록 공공 가상머신과 같은 최적의 기술적 솔루션을 도입해야 한다. 만일 이러한 기술적 솔루션에 적절한 정책이 뒷받침된다면, 법제도와 기술적 대책이 상호보완하며 안전한 발전이 가능할 것으로 기대된다.

4.3.2 공공 와이파이 확대 정책

공공 가상머신을 이용하기 위해서는 안정적인 인터넷 환경이 필수적이다. 그러나 2020 글로벌 모바일 데이터 가격비교 현황(국회과학기술정보방송통신위원회)에 따르면 한국의 데이터 요금은 OECD 평균보다 3배 이상 높은 것으로 조사되었다. 범국가적인 공공 가상머신 환경을 구축하고 이를 활성화하기 위해서는 국민들에게 저렴한 인터넷 환경을 제공할 수 있어야 한다.

공공 와이파이 확대 정책의 한 예로 미국 뉴욕시는 2014년부터 모든 시민에게 인터넷에 대한 균등한 접근권을 제공하는 에퀴터블 시티(Equitable City)를 목표로 2024년까지 도시 전체를 커버하는 무선 네트워크(LinkNYC)를 완성하기 위한 프로젝트를 진행하고 있다.

4.3.3 공공 인프라 보안 강화

우리나라에서 운영되고 있는 공공 와이파이기는 공공재임에도 불구하고 일원화된 관리체계나 가이드라인이 존재하지 않아 각 기관에 의해 제각각 관리되고 있고, 이로 인한 보안 문제가 꾸준히 대두되고 있다[27]. 우리나라는 디지털 뉴딜 정책의 일환으로 공공 와이파이 신규 구축 및 노후 와이파이 품질 고도화 사업을 추진하고 있지만, 여전히 보안 대책이 미비한 실정이며 사업 추진에 있어서 기업 의존적인 태도를 보이고 있다. 사람들이 공공 와이파이를 안전하게 이용할 수 있도록 하기 위해서는 통합관리센터를 구축하여 보안 관리체계를 일원화하고, 안전한 공공 인프라 사용을 위한 표준 가이드라인을 마련하여야 한다.

4.4 기대효과

공공 와이파이 확대 정책과 공공 가상머신의 도입으로 디지털 빈부격차로 인한 양극화를 해소하고, 보안 사고 및 보안 위협에의 노출을 줄일 수 있을 것으로 기대한다.

본 연구논문에서 제안한 가상머신 기반의 공공 클라우드 기술과 정책을 활용하면 누구나 인터넷이 가능한 단말을 이용해 언제 어디서나 쉽고 안전하게 공공 가상머신에 구축된 인프라와 애플리케이션을 활용할 수 있어 양극화를 개선할 수 있다. 교육기관에 공공 가상머신이 도입될 경우, 학생들은 가지고 있는 PC의 사양과 관계없이 수업을 수강할 수 있어 비용적 부담을 줄일 수 있다. 그리고 교육자 및 교육기관은 학생의 PC 환경을 보다 쉽게 파악할 수 있으며, 학생들의 수강 환경이 일정 수준 이상이라는 것을 전제로 교육을 제공할 수 있게 되므로 질 좋은 수업을 제공할 수 있다. 그리고 공공 서비스에 공공 가상머신이 도입될 경우, 고령층을 대상으로 하는 건강 취약계층 스마트 건강관리 등의 서비스 이용을 위한 소프트웨어 설치 등의 복잡한 과정이 이미 완료된 환경을 공유하여 디지털 소외계층이 겪을 수 있는 어려움을 해소할 수 있다.

공공 가상머신을 데이터 활용 및 관리 플랫폼으로 사용한다면 디지털 자산에 대해 원 소스 멀티 유즈(one source multi use)가 가능해져 자원을 효율적이고 편리하게 활용할 수 있다. 이를 통해 사용자는 디지털 인프라와 애플리케이션을 저렴하고 편리하게 이용할 수 있으며, 원하는 시간에 필요한 자원을 할당받아 혜택을 누릴 수 있다. 그리고 데이터 활용 활성화를 위한 도구로 공공 가상머신을 채택한다면, 효율적이고 편리하게 기관 간 협업을 도모할 수 있고, 안전하게 공공 서비스를 제공할 수

있다. 전문 인력으로 구성된 전담 기관이 공공 가상머신을 관리하고 통제하므로 보안 관리가 어려운 개인 컴퓨팅 환경보다 안전하게 사용 가능하다. 그리고 데이터 불법 복제 및 데이터 유출 방지 등의 관리가 용이하며, 보다 저렴하게 데이터의 보안성을 향상시킬 수 있다. 공공 가상머신으로 데이터 관리 및 공공 서비스 제공 플랫폼을 사용한다면, 디지털 비대면 공공 서비스 운영 중에 발생하는 보안 사고에 대응하기 위하여 다른 협업 도구 제공 기업이나 보안 기업에 중요 정보를 공유할 필요가 없고 대응 절차를 줄일 수 있으므로 보안 사고 대응 속도를 향상시킬 수 있다.

개인 또는 기업은 이미 구축된 공공 가상머신 환경을 활용해 효율적으로 디지털 비즈니스 테스트베드를 시험할 수 있고, 아이디어 기반의 혁신 창업 친화적 환경을 조성할 수 있다. 전 세계가 탈세계화와 신민족주의 시대로 발전하고 있는 가운데, 공공 가상머신을 통해 아이디어 기반의 창업 환경을 뒷받침하고 디지털 자산 거래 시장을 선점한다면, 포스트 코로나 시대에 디지털 경제를 선도할 수 있을 것이다.

5. 결론

지능화, 가속화되는 정보화시대에 업무의 효율성, 유연성 등의 확보를 위하여 행정기관 등의 업무에 공공 클라우드의 도입이 확대되고 있다. 또한, 정부는 디지털 전환 가속화를 위한 각종 정책을 펼치며 전자 정부로서의 입지를 다지고자 한다. 그러나 급격한 환경 변화에 따른 양극화 심화와 보안 사고에 대한 우려가 제기되고 있다.

본 논문에서는 빠르게 변화하는 세상을 선도하고 국가적 안정을 취하기 위하여 종래 법령 및 기술 분석을 통해 새로운 정책적·기술적 방안을 제안하였다. 종래 지침 및 법령은 디지털 전환의 사각지대에 놓인 계층에 대한 고려가 부족하며, 보안 규제를 완화하는 등 보안보다는 데이터 활용 활성화에 더욱 초점을 맞추고 있다. 이 허점을 보완하지 않은 채로 전 공공 행정 업무에 공공 클라우드가 도입된다면, 기존에 제기되었던 우려는 더욱 심화될 것이며, 국민의 개인정보 유출 사례는 증가하게 될 것이다.

이에 본 논문은 종래의 클라우드 기술과 정책의 한계점을 분석하고 공공 클라우드와 공공 와이파이 기반의 범국가적 공공 가상머신의 구축 및 활성화를 위한 기술 개념과 정책 방향을 제안하였다. 공공 가상머신이 구축 및 도입되어 공공 클라우드와 함께 공공 행정 업무에 활

용된다면 향상된 보안성과 함께 업무의 효율성 및 유연성을 보장할 수 있을 것이다. 또한, 공공 가상머신이 민간 영역으로 확대 적용된다면 대한민국은 IT 선도국가로 거듭남은 물론이고 균형적 국가 발전을 통해 디지털 사회 혁신을 이룰 수 있을 것이다.

REFERENCES

- [1] I. S. Baek. (2021). Major issues and policy directions in the digital sector in 2021. *The Journal of The Korean Institute of Communication Sciences*, 38(2), 3-11.
- [2] Government agency. (2020). Digital new deal comprehensive plan.
- [3] Government agency. (2020). Digital government innovation in the post-corona era.
- [4] J. S. Park & J. Y. Kim & E. J. Kim. (2019). A Study on Open Cloud Platform Application Model for Public Sector Collaboration Environment. *Proceedings of Symposium of the Korean Institute of communications and Information Sciences*, 429-430.
- [5] K. K. Kim & J. H. Na & P. U. Jeong. (2019). A Study on Introduction and Improvement of Cloud Computing Service in Public Sector: Focused on Certified IaaS. *Journal of Information Technology and Architecture*, 16(3), 273-280.
- [6] S. Y. Park & J. W. Kim. (2019). A Panel Analysis (2010-2018) of the Digital Divide among Different Age Groups among Older Adults. *Journal of The Korean Data Analysis Society*, 21(5), 2,407-2,418.
- [7] S. D. Sik. (2019). *The Report on the Digital Divide 2019*. Seoul:NIA.
- [8] C. K. Jang & U. J. Seong. (2020). The Effect of Digital Divide on the Use of Online Services in the Severely Disabled People: Focusing on Online Accessibility. *Informatization Policy*, 27(3), 56-81.
- [9] Y. U. Lim. (2020). *What are the promising techniques for preparing for the post-Covid-19 era?*. Sejong:MSIT.
- [10] Toqeer Mahmood & Tabassam Nawaz & Aun Irtaza & Rehan Ashraf & Mohsin Shah & Muhammad Tariq Mahmood. (2016). Copy-Move Forgery Detection Technique for Forensic Analysis in Digital Images. *Mathematical Problems in Engineering*.
- [11] IGLOOSecurity. (2020). *Threat technology outlook report*. Seoul:IGLOOSecurity.
- [12] IBM Security. (2020). *2020 Data leakage cost report*. New York:IBM.
- [13] K. H. Park. (2020). A Study on the Balanced National Development in the Post-Corona Era. *PLANNING AND POLICY*, 5-10.
- [14] H. G. Oh. (2020). Analysis of major social changes and information security issues after COVID-19. *Communications of the Korean Institute of Information Scientists and Engineers*, 38(9), 48-56.
- [15] Y. M. Jeong & S. O. Choi. (2019). The Effect of E-government on Digital Divide. *Journal of Korea Technology Innovation Society*, 22(5), 942-961.
- [16] KISA. (2020). *Cloud Services Security Certification System Operational Change Management Sheet*. Seoul:KISA.
- [17] CVE Details. (2019). *Vulnerabilities By Year*. CVE Details(Online). <https://www.cvedetails.com/browse-by-date.php>.
- [18] D. M. No. (2020). *A Study of Plans for an Innovative Inclusive State: Social Security Policies*. Sejong: A society of economic and humanities.
- [19] NIA. (2019). *2019 E-Government Service Usage Survey Results Summary Report*. Daegu: NIA.
- [20] MSIT. (2020). *2020 Cloud Industry Survey Results Report*. Daegu: MSIT.
- [21] NIA. (2021). *Information Use*. Digital Services Market Seed. <https://www.ceart.kr>
- [22] NIA. (2021). *Introduction to NIA Features*. NiCloud. <https://nicloud.kr>
- [23] PaaS-TA. (2021). *Introducing PaaS-TA*. PaaS-TA. <https://www.paas-ta.kr>
- [24] Joint with relevant ministries. (2020). *Cloud Industry Evolution Strategy*. Seoul : Presidential Committee on the 4th industrial revolution.
- [25] Y. H. Sim, H. G. Lee. (2018). *Cloud Computing Technology Trends*. Seoul : COMPA.
- [26] PIPC. (2020). *Guidelines for processing pseudonym information*. Seoul : PIPC.
- [27] Legislative Investigation Agency of the National Assembly. (2019). *Status and improvement of public Wi-Fi construction and operation*. Seoul : Legislative Investigation Agency of the National Assembly.

김 소 희(Kim So-Hui)

학사학위



· 2018년 2월 ~ 현재 : 성신여자대학교
융합보안공학과
· 관심분야 : 융합보안, 미래융합기술
· E-Mail : 20180903@sungshin.ac.kr

이 유 림(Lee Yu-Rim)

[학생회원]



- 2018년 2월 ~ 현재 : 성신여자대학교 융합보안공학과
- 2020년 9월 ~ 현재 : 성신여자대학교 미래융합기술공학과 (학석사 연계과정)
- 관심분야 : 융합보안, 인공지능 보안
- E-Mail : 20180940@sungshin.ac.kr

이 일 구(Lee Il-Gu)

[정회원]



- 2003년 2월 : 서강대학교 전자공학과 (공학사)
- 2005년 2월 : 한국과학기술원 정보통신대학원 (공학석사)
- 2012년 2월 : 한국과학기술원 지식재산대학원 (경영학석사)
- 2016년 2월 : 한국과학기술원 정보보호대학원 (공학박사)
- 2005년 2월 ~ 2017년 2월 : 한국전자통신연구원 5G기가통신시스템연구본부 선임연구원
- 2017년 3월 ~ 현재 : 성신여자대학교 융합보안공학과/미래융합기술공학과 조교수
- 관심분야 : 융합보안, 미래융합기술
- E-Mail : iglee@sungshin.ac.kr