논문 2022-2-14 http://dx.doi.org/10.29056/jsav.2022.12.14

국가 주요 기반시설 대상 안전한 클라우드 분석에 관한 연구

서대희*†

A Study on Secure Cloud Analysis for National Infrastructure

Daehee Seo*†

요 약

최근 발달되고 있는 클라우드는 AI, 블록체인을 비롯한 타 기술 및 산업과 융합되고 있으며, 온·오프라인의 대부분의 서비스가 클라우드로 구성되고 있다. 이는 민간분야를 넘어 국가 주요기관 및 공공기관에서 많이 활용되고 있다. 하지만 클라우드 환경에서, 데이터 활용 시, 데이터 유출, 손실 등 다수의 보안 위협이 발생할 수 있다. 만약 클라우드에 활용되는 데이터가 사용자들의 민감한 정보나, 혹은 주요기관에 의해 중요한 정보라면, 노출시 다양한 보안 위협으로 인해 상당한 피해가 예상된다. 본 논문은 국가 주요 기반시설을 대상으로 안전한 클라우드 아키텍쳐 솔루션를 위한 기술 동향 및 조사에 관한 것으로, 각 주요국의 클라우드 정책에 대한 조사와 국내에서 추진 중인 클라우드 정책에 대해 설명한다. 그리고 조사한 자료를 기반으로, 국가 주요 기반 시설에 사용될 클라우드를 안전하게 구성하기 위해 고려해야할 방향이나 기술, 요구사항 등을 제언한다.

Abstract

The recently developed cloud is converging with other technologies and industries including AI and blockchain, and most online and offline services are composed of the cloud. It is widely used in major national and public institutions beyond the private sector. However, there are various security threats such as data leakage and loss when using data in a cloud environment. If sensitive information of users or important information is shared in the cloud, significant damage is expected when exposed to security threats. This paper is about technology trends and research for secure cloud architecture solutions for major national infrastructures. A survey on cloud policies in each major country and cloud policies being promoted in Korea will be explained. And based on the researched data, we suggest the direction, technology, and requirements to consider to securely configure the cloud to be used for major national infrastructure.

한글키워드 : 클라우드, 접근제어, 보안기술, 보안 정책, 클라우드 보안인증제도

keywords : ITS, Access Control, Security Technology, Security Policy, CSAP

1. 서 론

최근 발달되고 있는 클라우드는 AI, 블록체인을 비롯한 타 기술 및 산업과 융합되고 있으며, 온·오프라인의 대부분의 서비스가 클라우드화되고 있다. 1세대 클라우드 인프라가 스토리지, 컴퓨팅 파워 등에 의존했다면, 2세대 클라우드 인

* 상명대학교 지능데이터융합학부
† 교신저자: 서대희(email: daehseo@smu.ac.kr)
접수일자: 2022.09.15. 심사완료: 2022.09.26.
게재확정: 2022.12.20.

프라는 플랫폼, 소프트웨어에 의존되고 있으며, 3세대는 AI, AR·VR, IoT 등 서비스화 되는 모든 기술들이 클라우드 인프라가 되고 있다[1]. 코로나 19 이후 온라인 교육, 재택근무 등 우리 주변에서 클라우드를 활용한 요소들을 흔히 볼 수 있다. 현재는 민간분야를 넘어 국가 주요 기관 및 공공기관에서 많이 활용되고 있다. 하지만 클라우드를 사용하여, 데이터 활용시, 데이터 유출, 손실을 비롯하여, APT, 불충분한 인증 및 접근관리 등 다수의 보안위협이 발생할 가능성이 존재한다. 만약 클라우드에 사용자들의 민감한 정보나, 혹은 주요 기관에 의해 중요한 정보가 공유된다면, 보안 위협 노출시 상당한 피해가 예상된다. 따라서, 클라우드 활용시 보안에 대한 대응책이 고려되어야 한다. 특히 국가 주요 기반시설, 공공기관에서 사용될 클라우드는 안전한 클라우드 서비스가 기반이 되어야 한다.

해외 주요국 중 미국은 '18년 기존의 "CLoud only"정책을 "Cloud Smart Strategy"로 전환하여, 클라우드 확산시 장애가 될 수 있는 보안규정을 완화하였으며, 공공클라우드 서비스에 미국 정부 정보기관에서 기밀 수준으로 분류되는 SW 및 데이터를 사용하였다.

국내에서도 제 3차 클라우드 기본계획('22~'24년)을 발표하여, 공공부문의 클라우드 전면 전환을 추진하고 있으며, 민간클라우드를 공공기관에 활용하기 위해 보안인증제도 시행 및 정보보호 기준고시, 가이드라인을 마련중이다[2]. 또한 '22년에 "국가 사이버안보 강화를 위한 미래 유망 정보보안기술 전망 보고서"를 발간하였으며, 다수의 미래 유망 정보보안 기술 중 국가 클라우드 보안에 대해 고려하고 있다[3].

본 논문은 국가 주요 기반시설을 대상으로 안전한 클라우드 아키텍처 솔루션를 위한 기술 동향 및 조사에 관한 논문이다. 논문에서는 미국을 비롯한 주요국의 클라우드 정책에 대한 조사와 국내에서 추진 중인 클라우드 정책에 대해 설명할 것이다. 그리고 이를 기반으로, 향후 국내에서 추진중인 주요 기반 시설을 대상으로 사용되는 클라우드 아키텍처를 안전하게 구성하기 위해 고려해야할 방향을 제언한다.

2. 국내 · 외 클라우드 기술 동향

2.1 클라우드 컴퓨팅

클라우드 컴퓨팅은 네트워크 환경에서 서버를 이용하여, 데이터 저장 및 관리, 콘텐츠 사용 등의 다양한 서비스를 제공받을 수 있으며, 시간 및 장소의 제한 없이 필요한 만큼의 컴퓨팅 자원을 활용할 수 있다. 사용자가 IT 자원을 직접 관리 및 소유하는 기존의 방식과 비교하여, 사용자가 인터넷을 통해 필요한 IT 자원을 클라우드 제공자로부터 제공받을 수 있다[4]. 4차 산업혁명에서 클라우드는 빅데이터와 인공지능의 역할의 중요성이 증대됨에 따라 기반이(기초가)되는 인프라로 부각되었다. 특히 자본력이 부족한 스타트업이나 중소기업은 클라우드를 통해 대규모 컴퓨팅 자원을 저렴하게 활용할 수 있다[5]. 포스트 코로나 19 상황인 오늘날 온라인 교육, 재택근무 등 우리 주변에서 클라우드 활용하는 사례는 흔히 볼 수 있다. 나아가 서론에서 언급한 것 같이 국가 주요 기반 시설 및 산업이나 공공기관 분야에 클라우드 사용을 전면 확산하는 추세이다.

클라우드 컴퓨팅은 서비스 유형과 운용형태에 따라 [표 1], [표 2]와 같이 구분된다[6].

2.2 클라우드 시장 동향

글로벌 클라우드 시장은 '20년 2,130억 달러에서 '25년 5,042억 달러로, 연 19.3%씩 증가할 것으로 전망하였다[7]. PaaS 시장은 '20년 448억 달러에서 '25년 1,544억 달러로, 연 29.5%씩 증가할

표 1. 클라우드 서비스 유형
Table 1. Cloud service type

구분	설명
IaaS (Infrastructure as a Service)	사용자에게 스토리지, 서버 등의 하드웨어 자원을 제공·임대해주는 서비스 (예: S3, EC2, Amazon 등)
PaaS (Platform as a Service)	사용자에게 SW 개발시 필요한 플랫폼을 제공·임대해주는 서비스 (예: PHP, Linux, MySQL, Apache 등)
SaaS (Software as a Service)	사용자가 원하는 SW를 제공·임대해주는 서비스 (예: iCloud, 웹메일 서비스 등)

표 2. 클라우드 운용형태
Table 2. Cloud operation type

구분	설명
Private Cloud	• 클라우드 서비스 환경을 기관 및 기업 내부에 구성하고, 내부 사용자에게 서비스를 제한적으로 제공하는 형태
Public Cloud	• 불특정 다수의 사용자를 대상으로 하는 서비스 형태
Hybrid Cloud	• 프라이빗 클라우드와 퍼블릭 클라우드를 결합한 형태 • 프라이빗 정책을 설정한 후 공유를 원하지 않는 민감·중요한 서비스 및 일부 데이터에 대한 서비스를 제공
Multi Cloud	• 클라우드 공급업체들 중 2곳 이상의 공급업체에서 제공되는 2개 이상의 프라이빗 또는 퍼블릭 클라우드로 구성된 클라우드

것으로 전망하였다. SaaS 시장은 '20년 1,682억 달러에서 '25년 3,498억 달러로 연 16.3%씩 증가할 것으로 전망하였으며, Public Cloud 시장은 '20년 PaaS(16.0%), SaaS(59.9%), IaaS(24.1%) 순으로 나타나고 있다. '25년까지 PaaS(20.6%), SaaS(46.8%), IaaS(32.6%)으로 증가할 것으로 전망하였다[7]. 대부분의 기업들이 클라우드를 활용하는 목적은 비용 절감에서 빅데이터, 인공지능 적용할 수 있는 인프라로 활용할 수 있기 때문이다. Google, Amazon, MS과 같은 글로벌 기업은 IaaS를 넘어 머신러닝 엔진과 함께 번역, 사진·동영상 인식, 음성인식과 같은 자체 API를 공개함으로써 PaaS로 진화하였다. 클라우드 시장을 압도적으로 AWS가 점유하는 가운데 Alibaba, MS, Google가 빠르게 성장하고 있다[7].

일본 시장조사기관 엠엠종합연구소(MM Research Institute)의 '19년 클라우드 서비스 수요 동향 조사에 따르면, '18년 일본의 클라우드 서비스 시장 규모는 약 1조 9,000억엔으로 2017년 대비 22.7% 증가한 것으로 나타났다. 엠엠종합연구소에 따르면 일본의 클라우드 시장은 '18년부터 매년 평균 18.9%씩 증가하여 '23년에는 약 4조 5,000억 엔이 될 것으로 예상된다[8].

중국 클라우드 컴퓨팅의 '21년 시장규모는 3,229억 위안(약 62조원)으로, 전년 대비 약 54.4% 증가한 수치이다[9]. 허바오훙(何寶宏) 중국정보통신연구원 빅데이터 및 클라우드 컴퓨팅 연구소 소장은 "향후 몇 년 동안 중국 클라우드 컴퓨팅 시장이 연간 약 30~40%의 성장률을 보일 것"이라고 발표했다. 이를 기반으로 '25년 시장 규모가 1조 위안(195조6천600억원)에 도달할 것"이라고 전망했다.

국내 클라우드 시장은 '20년 7,204억원에서 '25년 1조 5,177억원으로, 연 16.5%씩 증가할 것으로 전망하였다. SaaS와 PaaS 시장은 각각 '25년까지 연평균 14.9%, 22.9%씩 증가해 1조 1,432억원, 3,825억원에 도달할 것으로 전망하였다. Public Cloud 시장은 '20년 PaaS(9.7%), SaaS(39.3%), IaaS(51.0%) 순으로 나타나고 있으며, '25년까지 PaaS(11.9%), SaaS(36.5%), IaaS(51.6%)으로 증가할 것으로 전망하였다[7]. 다양한 형태의 워크로드(보안, 비용, SALs 등)에 따라 자체 IT 환경 및 외부 클라우드가 혼재되어 활용되는 하이브리드 클라우드가 확산될 것으로 전망하였다. 국내 시장을 Google, AWS, MS 등 해외 클라우드 사업자가 주도하는 가운데 네이버, KT 등이 퍼블

릭 클라우드 IaaS 시장에서 시장 점유율 일부를 확대하였다. 그 외 다양한 업체들이 자체 보유 기술력을 기반으로 특화된 클라우드 서비스 및 솔루션을 제공하며 시장 경쟁력을 확보하였다[7].

Gartner, IDC는 '20년도 유망 기술 및 '20년도 Top 10 전략적 기술 트랜드로 엣지컴퓨팅, 분산·멀티클라우드 기술을 선정하고 서버리스 및 컨테이너 기술의 사용 확산을 전망하였다[10]. 주요 클라우드 기업은 타 기업과의 협력 및 분산·멀티 클라우드 분야의 기술 개발을 통해 경쟁력을 지속적으로 강화하며 시장을 지배하였다. 글로벌 클라우드 선도기업은 서비스 경쟁력, 압도적 기술우위 등을 내세워 국내 클라우드 시장을 조금씩 잠식하려는 추세이다. 글로벌 기업 MS, GE, 아마존(AWS) 등은 클라우드 환경에 IoT, AI, 빅데이터 등을 융합하고, 산업 전반(의료, 금융, 제조, 교육 등)에 클라우드를 확산하고 있다[7].

'18년도 ICT 기술 수준 조사 자료에 의하면, 최고기술국(미국)과 비교하여, 한국은 16.0%의 기술수준 격차를 보인다. 국가별로는 미국(100%)과 비교하여, 유럽(10.7%), 중국(15.0%), 일본(15.8%), 한국(16.0%)을 유지하고 있는 것을 알 수 있다[11]. 즉, 한국의 클라우드 기술수준은 증가하고 있으나, 중국의 상승세보다 느리다. 클라우드 엣지 및 멀티 클라우드와 관련하여 일부 기업을 중심으로 연구개발 및 정부 R&D을 추진하였나, 기술 수준이 가장 낮은 것으로 분석되었다[7].

2.3 클라우드 표준화 현황

현재 미국을 비롯한 주요국들은 기술 진화에 따라 클라우드 기본 표준화에서 기술 고도화 표준 개발을 추진 중이다. PG1003(TTA 클라우드 컴퓨팅 프로젝트 그룹)에서 클라우드 융합 및 기반 기술, 응용 분야에 대한 단체표준을 제정하였다. 국제표준화기구인 ISO/IEC SC 38(클라우드 컴퓨팅 및 분산 플랫폼), JTC 1(정보기술)에서는 클라우드 정의 및 구조 등의 국제표준을 제정하였다. 국제전기통신연합 ITU-T는 클라우드 기반 보안 기술 및 네트워크 관련 국제표준을 개발·제정하고 있다. 미래네트워크 및 클라우드 환경에서 SG 13는 클라우드 네트워크 가상화, 서비스 요구사항, 컨테이너 프레임워크 등의 표준 기술 개발에 대한 내용을 포함하며, 클라우드 보안 측면에서 SG 17는 인프라형 서비스 보안 요구사항 및 네트워크 등의 보안 표준 기술 개발 내용을 포함한다[7].

3. 클라우드 정책 동향

3.1 주요국의 클라우드 정책 동향

'15년 이전 ICT 패러다임이 클라우드로 변화됨에 따라 미국을 포함한 클라우드 주요 선진국들은 공공부문에서 우선 주도를 통해 민간 클라우드 확산을 추진하였다.

미국은 기존의 클라우드 전략(Cloud Frist and Cloud Only)에서 클라우드 확산 정책 고도화를 위해 연방정부 클라우드 전략(Cloud Smart)을 '19년도에 발표하였다. 이 시점에 특정 벤더 의존성 완화하기 위해 공정 조달을 수행하고, FedRAMP를 통해 SaaS 신속 인증 및 인력교육(재교육), 비즈니스 지속성 등을 강조하였다. '18년 대비 소프트웨어 개발, 클라우드 서비스, 연방정부의 사이버 보안에 대한 지출이 약 6% 이상 증가하였다. '20년 CIA는 내부의 SW 시스템을 개선하기 위해 PaaS와 SaaS를 도입 하였다[7].

영국은 클라우드 이용 활성화를 위해 '11년도 3월에 공공조달 거버넌스 구축을 진행하였으며, '12년 2월에 '클라우드 스토어'를 개설하여 공공부문의 클라우드 이용을 촉진하였다. 이때 당시 19,553개 서비스가 약 2천여 기업의 스토어에 등

록되었다. '16년에는 정부 정보화 예산의 10%인 1.1조원을 클라우드에 활용하였으며, 민간 클라우드에서 공공 데이터의 90% 이상을 사용 가능하도록 개편하였다. 디지털서비스 전문계약제도 운영 및 유통 마켓 제공을 통해 공공부문 유통활용을 촉진하고, Public Cloud First 정책을 '17년에 추진하였다[12].

'13년 유럽은 클라우드 ICT 시장을 세계 최대 규모로 만들기 위해 국가적 장벽 해소 방안, 공공 조달력 활용 등을 검토하였다. 특히 '18년에 로드맵(PICSE) 수립하고, 하이브리드 멀티 클라우드, 보안 등의 선결 조건을 포함한 조달 거버넌스를 수립하여, 클라우드 네이티브 패러다임으로 전환하기 위해 노력하였다. '20년에는 클라우드 합의문에 27개 EU 회원국이 서명을 하여, 효율적인 차세대 클라우드 구축에 공동으로 투자하기로 하였다. 이를 기반으로, '21년 유럽 클라우드 얼라이언스가 39개 기업으로 구성되어 창설됐다[13].

'10년 일본은 13개 중앙정부의 ICT 자원을 1개의 클라우드로, 지자체는 3개의 클라우드로 통합 추진하였다. '13년 추진된 가스미가세키(霞が關) 프로젝트로 지자체·중앙부처에 클라우드 도입이 지원되었다. 일본 정부는 IT신전략을 통하여 디지털 기술 적용을 통한 중앙과 지방, 민과 관의 범주를 넘는 디지털 거버넌스 실현을 바탕으로 사회적 문제의 해결과 경제 성장을 목표로 하고 있다. 일본 정부는 '20년 향후 4~8년 동안 AWS의 클라우드에 자체 개발한 20개의 핵심 정부 시스템을 이전하기로 발표하였다[8]. '23년까지 지방자치단체 행정의 클라우드화 도입을 목표로 모든 지방자치단체의 민관데이터 활용 추진계획을 수립하고 있다. 해당 프로젝트를 통하여 정부 및 지방단체의 운영비용은 기존 시스템과 비교하여 약 30%이상 절감될 것으로 예상된다.

중국은 '15년 1월 6대 핵심전략(기업 혁신역량 제고, 전자정부 발전, 클라우드 서비스 공급 능력 강화(민간 클라우드 발전), 클라우드 인프라 시설 구축, 빅데이터 개발 및 이용 강화, 안전보장 강화)을 발표하여 세계 수준의 클라우드 실현을 목표로 하였다. 그리고, 자국 내에 클라우드 데이터 센터를 두기 위해 인터넷 안전법을 발표하였다. '17년에는 클라우드 컴퓨팅 발전 3개년 계획('17~'19년)을 발표하여, 중국 클라우드 시장을 '21년까지 71조원으로 기업 경쟁력 강화 및 육성을 추진하였다[2]. 주로 SW기업에서 클라우드로 환경으로 빠른 전환을 지원하고, 공공서비스 플랫폼을 건설하며, 무엇보다 클라우드 핵심기업 육성이 목표였다.

3.2 국내 클라우드 정책 동향

현재 정부는 제 1차·제 2차 클라우드 기본계획을 수립하고, 정책적 노력 등을 통해 산업·공공의 클라우드 이용 기반을 조성하였다[1].

- 제 1차 기본계획('16~'18)를 통해 중소기업 클라우드 이용 지원, 클라우드 보안 인증제 신설 등 산업성장 기반 마련
- 제 2차 기본계획('19~'21)를 통해 주요 분야별 클라우드 서비스 개발, 지차제·중앙부처의 민간 클라우드 확산 허용 등 클라우드 활용 사례를 확산시키는데 집중

그리고, 이를 기반으로 산업, 공공분야를 비롯한 전 분야에 클라우드 이용을 전면적으로 확산하기 위해 '21년 제 3차 클라우드 기본계획을 발표하였다. 제 3차 클라우드 기본계획은 목표는 전면적으로 국가 클라우드 전환을 통해 인공지능과 데이터의 경제를 가속화하고, 정책 방향 마련 추진 등으로 디지털 선도국가로 도약하기 위함이다. 현재, 공공부문에서의 민간 클라우드를 전환하는 단계는 아직 초기 단계이기 때문에, [표 3]과 같이 발표된 추진전략 및 과제 등을 통해 6대 공공분야 클라우드 혁신 추진하고 있다. 나아가

공공기관, 국가 주요 기반 시설로 확장을 목표로 하고 있다[1].

표 3. 추진전략 및 과제[1]
Table 3. Promotion strategy and tasks

추진전략	과제
공공부문 민간 클라우드 우선 이용	1. 민간 클라우드 이용 지원체계 마련 2. 공공부문 민간 클라우드 도입 촉진 3. 민간 클라우드 도입을 위한 조달체계 혁신 4. 안전한 민간 클라우드 이용환경 조성
클라우드 산업 경쟁력 강화	1. SW 산업의 SaaS 전환 2. 산업 전반의 클라우드 이용 확산 3. 클라우드 서비스 글로벌 진출 확대
클라우드 산업 지속성장을 위한 생태계 조성	1. 플랫폼 생태계 조성을 통한 경쟁력 강화 2. 기업 맞춤형 인재 양성 3. 클라우드 기반 인공지능 연구 지원체계 강화 4. 데이터 센터 확충 및 운영 효율화

4. 국가 주요 기반 시설에 사용되는 클라우드 동향

4.1 클라우드 보안위협

클라우드 컴퓨팅은 자원의 공유를 비롯해 가상화 기술 적용, 정보의 외부위탁, 다양한 단말기의 접속이 가능한 특징을 가지고 있다. 하지만 이러한 특징으로 인해 클라우드 컴퓨팅 환경에서 다양한 보안 위협이 발생할 수 있다. 따라서, 클라우드를 사용하는 사용자와 서비스 제공자는 클라우드 활용시 발생할 수 있는 보안 위협을 정확히 인식하고, 이러한 보안 위협이 최소화 될 수 있도록 반드시 주의가 요구된다. 클라우드 환경에서 발생할 수 있는 보안 위협들은 CSA(Cloud Security Alliance)를 중심으로 '10년, '13년, '16년, '19년 지속적으로 발표되고 있다. 클라우드 컴퓨팅은 '10년 7대 위협으로 시작해, '13년에는 9대 위협, '16년에는 12대 위협, '19년에는 13대 보안위협이 존재한다. 대표적인 보안위협은 다음과 같다.

- 악의적인 내부자들
- 클라우드 컴퓨팅 남용과 악의적인 사용
- APT, 불충분한 인증 및 접근관리
- 불충분한 심사
- 안전하지 않은 API
- 데이터 유출
- 트래픽 및 서비스 탈취
- 계정도용
- 서비스 거부(DoS)
- 데이터 손실, 시스템 취약점
- 공유기술 취약점,
- 스펙트라 멜트다운

클라우드 서비스 이용이 확대됨에 따라 클라우드 환경에서의 보안위협도 기술적, 관리적 범위에서 점차 늘어나고 있기 때문에, 이에 대한 대응방안이 필요하다.

4.2 안전한 클라우드 아키텍처

국가 주요기반시설에 사용될 클라우드의 경우 안전한 클라우드 아키텍처를 위한 솔루션이 제공되어야 한다. 하지만 현실은 보안 기술을 적용한 아키텍처보다 안전한 클라우드 환경을 위한 인증제도뿐이다[14]. 클라우드컴퓨팅 보안인증제도는 사용자들이 클라우드컴퓨팅 서비스를 이용시 안심하고 도입·사용할 수 있도록 한국인터넷진흥원(KISA)에서 제공받는 서비스가 “클라우드컴퓨팅 서비스 정보보호에 관한 기준”을 준수하는지의 여부를 객관적으로 인증·평가해주는 제도이다. 클라우드컴퓨팅 보안인증은 서비스 제공자의 의무사항이 아니다. 하지만, 공공기관과 같이 중요

한 데이터를 활용하고자 하는 환경에서는 반드시 필요하다. 클라우드 보안인증을 받기 위해 한국인터넷진흥원에 신청하여야 하며, 대략적으로 소요시간은 준비에서 인증까지는 3~6개월이 걸린다. 정보보호관리체계(ISMS)와 비교하여, 현장점검 및 문서점검 외에 취약점 점검, 모의침투 테스트 등 기술점검을 실시한다. 또한 공공기관에서 제공해야 할 요구사항을 추가할 수 있다[15][16].

이 외에 서비스 제공자가 클라우드 서비스를 공공기관에 제공하기 위해서는 국가정보원이 지정한 인증기관에서 정보보호제품(CC인증 필수제품)에 대해 CC인증을 받아야 한다. 공공기관용 추가 보호조치 14.1.2., 클라우드 컴퓨팅 서비스 정보보호에 관한 기준에 따라 도입되는 정보보호제품, 가상화 솔루션 및 서버·PC 중에 필수적으로 CC인증을 받아야 하는 제품군은 국내·외 CC인증을 받은 제품을 사용하여야 한다. 클라우드 보안인증 외에도 「전자정부법 시행령」 제69조 및 '암호모듈 시험 및 검증지침'에 따라 자사가 제공하는 특정 하드웨어, 펌웨어, 소프트웨어 등에 대해서 암호모듈 검증을 받아야 한다[15].

4.3 미국 주요 기반 시설에 사용되는 클라우드 방향

미국에서 클라우드 컴퓨팅 환경에서 보안 및 법적 문제는 데이터 보호 지침에 따른 정보 조직의 주요 관심사이다[17]. 미국 정보는 행정 명령 135261에 설명된 국가 보안 정보에 대해 3단계 분류체례를 사용하였다[18]. 정보가 공개될 경우 국가 안보에 미칠 수 있는 영향을 고려하여 제안된 것이다.

- 기밀(Confidential): 무단 공개(unauthorized disclosure)가 국가 안보에 피해를 줄 것으로 합리적으로 예상되는 정보
- 비밀(Secret): 무단 공개가 국가 안보에 심각한 피해를 줄 것으로 합리적으로 예상되는 정보
- 일급비밀(Top Secret): 무단 공개가 국가 안보에 예외적으로 심각한 피해를 초래할 것으로 합리적으로 예상되는 정보

세부적으로, 미국 정부에서 활용하기 위한 클라우드 아키텍처가 되기 위해 [표 4]의 요구사항을 만족해야 한다. 이 외에 '20년 미군 클라우드 전략(The Army Cloud Plan)을 통해 인공지능의 중추인 클라우드를 통한 현대화 전략의 극대화 방안을 마련하였다. 대표적인 전략으로는 데이터 기반 의사 결정 가속화, 현장 소프트웨어 사용 시간 단축, 보안 인증 프로세스 최적화, 클라우드 설계, 소프트웨어 개발 및 데이터 엔지니어링을 핵심 역량으로 확립, 예측 불가능한 환경에 적응하기 위한 소프트웨어 설계 및 IT 자산/비용 투명성 제공 등이 중요 전략요소이다[19].

미국은 FedRAMP이란 표준화된 보안평가 및 인증제도를 활용하여 미 정부기관이 사용하려는 클라우드 서비스 및 제품에 대한 지속적인 모니터링, 보안평가, 허가 등을 수행한다. FedRAMP의 보안 인증 프로세스는 먼저 보안평가 수행 후 운용 권한 부여하고, 인증후 유지 및 지속적 평가, 총 3단계로 이루어지며, 평가대행기관에 선정되어야 인증 프로세스를 수행할 수 있다[20].

4.3 국내 주요 기반 시설에 사용되는 클라우드 방향 및 제언

서론에서 언급해듯이, 공공부문의 클라우드 전환은 현재 초기 단계로, 인식 부족, 재정적·제도적 지원 미흡 등으로 클라우드를 국가 전반으로 확산하는데 한계를 느꼈다[1]. 이는 공공기관에서 사용할 수 있는 보안인증된 SaaS가 부족하며, IaaS 위주로 사용 편중되는 "서비스 부족"과 오

표 4. 성공적인 정부용 클라우드가 되기 위한 요구사항
Table 4. Requirements to be a successful government cloud

요구사항	설명
프라이버시 (Privacy)	• 데이터 보호법에 따라 정부 기관은 클라우드 서비스 이용 시 개인 식별 정보 유출 위험을 제거하기 위해 클라우드로 데이터를 보내기 전에 익명으로 처리해야함 • 각국 정부는 이미 SOA(Service Oriented Architecture)를 사용하고 있으므로 클라우드 서비스 공급자는 클라우드 시스템에서 사용하는 계정과 정부 기관의 내부 사용자 데이터베이스 간의 연결(링크)을 신중하게 관리해야 함
보안 (Security)	• 공급자는 언급한 보안 요구 사항을 보장할 책임이 있기에, 예상치 못한 보안 사고에 대처할 때 계약 및 서비스 수준 계약(SLA)에 명확한 정책을 작성해야 함
기밀성 (Confidentially)	• 민감한 정보를 처리, 저장 및 통신할 때 인증, 권한 부여, 구획화(compartmentalization)를 달성하기 위해 특정 조치를 사용해야 함
가용성 (Availability)	• 제공자의 서비스 변경, 제공자에 대한 서비스 거부 공격, 서비스 종료까지 불가피한 문제가 발생할 수 있음 • 이에 공급자는 처음부터 상호 운용성을 고려하는 것이 중요하며 공급자가 다른 공급자에게 서비스를 이전할 수 있는 능력을 갖는 것이 필수적임
규제 (Regulatorily)	• 대부분의 법률규정은 개인정보를 처리할 때 개인을 보호하고 데이터의 자유로운 이동과 관련이 있음 • '02년 연방 정보 보안 관리법(FISMA)은 정보 보안의 중요성을 강조하고, 각 미국 기관의 장이 정보 보안 위험을 허용 가능한 수준으로 줄이기 위한 정책 및 절차를 구현하도록 요구함 • 서비스 제공자는 FISMA를 준수해야함

랜 규제로 공공부문에서 민간클라우드 사용 경험이 부족하다. 그리고 디지털서비스 전문계약제도와 같은 정책·기술·제도 등의 인식 저조하며, 이는 “경험 부족”이 되는 이유다. 또한 지자체·중앙행정기관 내부업무의 민간 클라우드 사용이 제한되었기에, 민간클라우드를 적극적으로 활용함에 있어 “제도적 한계”가 있는 것도 하나의 이유다.

민간분야 주요정보통신기반시설이 클라우드 가이드 라인을 통해 안전하고 효율적으로 클라우드를 이용할 수 있도록 기준과 절차를 정하였다. 국가 주요 기반시설에서 사용되는 클라우드 가이드라인 적용대상은 “정보통신기반 보호법” 제 8조 1항에 의해 지정된 민간분야 주요정보통신기반시설이다[21]. 국가·사회적으로 주요정보통기반시설은 중요한 정보통신시설이기 때문에, 기반시설 관리기관은 클라우드 사용시 반드시 주의가 필요하다. 만약 국가 기반시설 관리기관이 클라우드 서비스를 주요정보통신기반시설에 사용하고자 할 경우, 국내에 클라우드 서비스 시설들이 제대로 구축되어야 한다. 세부적으로 국내에서 데이터가 저장·관리·처리되어야 하며, 정보보호관리체계인증(ISMS)이나 이와 비슷한 수준의 인증(국내 외 클라우드 인증 등)을 받은 클라우드 서비스를 사용하여야 한다. 기존 주요정보통신기반시설과 동일하게 클라우드 이용 시에도 기반보호법 內 보호가 가능하다는 것을 보장해야한다. 기반시설 관리기관은 관계 중앙행정기관와 검토·논의하여 기반시설에서의 클라우드 사용이 가능한지에 대한 종합적인 판단 및 결정을 해야한다.

국내 공공기관 및 주요 기반시설에서 민간클라우드를 우선으로 전환하는 방향을 잡고 있으며, 이와 관련된 법령 및 고시 제정되고 있다. 변경된 고시에는 행정기관 등의 장이 신설로 정보시스템을 구축하거나 관리·운영하는 정보시스템을 교체할시 안정성, 보안성, 비용 효율성 및 확장성 등을 종합적으로 고려하여 “클라우드 컴퓨

팅 서비스” 사용을 우선 검토해야 하는 것으로 되어있다. 본 고시의 “제 7조”는 안정성 기준으로, KISA의 클라우드 보안인증제(CSAP)를 받아야 CSP를 활용할 수 있다[17]. 국내의 CSAP를 미국의 FedRAMP를 비교하면, 통제 기준 분류체계 및 통제 타입(분야)에 많은 차이가 있다. CSAP의 통제 분야는 기존의 인프라 운영조직의 업무 분야를 나열해 놓은 것처럼 보이는데, FedRAMP의 경우는 보안 목표인 무결성, 기밀성, 가용성과 직간접적으로 연관된 키워드들로 나열되어 있다. 또한 FedRAMP가 ‘통제 대상’을 중심으로 분류되었다면, CSAP의 경우는 ‘보안 업무’ 중심으로 분류되어 있다[22]. CSAP 평가항목 수는 laas 기준 14개 분야 117개 항목으로 구성되어 있으며, FedRAMP 평가항목 수는 17개 분야 325개 항목으로 구성되어 있다. 즉, CSAP가 FedRAMP에 비해 통제항목이 보안등급에 따라 체계화되어 있지 못하기 때문에 취약하다. [표 5]는 클라우드서비스 유형에 따라 분류하였기 때문에, 통제항목 수는 보안등급과는 무관하다. 아마도, 공공기관에서 민간클라우드를 도입할 경우 가장 우려하고 고려해야할 점이 보안일 것이다. 내부에 저장된 민감한 데이터를 외부 클라우드에 노출시킨다는 것에 대한 두려움은 항시 존재한다. 하지만 무엇보다 중요한 문제는 클라우드에 저장된 데이터들이 보안등급에 대해 제대로 분류되지 못하다는 것이다[22]. 각 기관별로 별도의 기준을 가지고, 데이터의 기밀 등급 체계를 표기할 것으로 생각된다. 만약 각 기관별로 통일되지 않은 보안기준을 사용하게되면, 향후 클라우드 전환(민간클라우드로의 전환)에 있어 큰 변수가 될 수 있다. 따라서, FedRAMP에서, 보안 등급에 따른 보안조치를 활용하는 것을 기반으로, 클라우드 인증시, CSAP에 구성된 평가항목 외에 데이터의 민감도나 중요도에 따른 다양한 인증 등급 방식이나, 평가항목 등 포함되어야 할 것이다.

표 5. FedRAMP와 CSAP 평가요소 비교
Table 5. Comparison of FedRAMP and CSAP Evaluation Factors

FedRAMP	CSAP
1. 접근통제	1. 정보보호 정책 및 조직
2. 인식 및 교육	2. 인적보안
3. 감사 및 책임	3. 자산관리
4. 인증, 보안 평가	4. 서비스 공급망 관리
5. 구성 관리	5. 침해사고 관리
6. 비상 계획	6. 서비스 연속성 관리
7. 식별 및 인증	7. 준거성
8. 사고 대응	8. 물리적 보안
9. 유지 보수	9. 가상화 보안
10. 매체 보호	10. 접근통제
11. 물리적 환경 보호	11. 네트워크 보안
12. 계획	12. 데이터 보호 및 암호화
13. 인사보안	13. 시스템 개발 및 도입 보안
14. 리스크 평가	14. 공공부문 추가 보안요구사항
15. 시스템 및 서비스 취득	추가요소: 데이터 중요도, 민감도에 따라서, 보안등급을 구성되어야 하며, 이에 따른 평가항목이 필요함
16. 시스템 및 통신 보호	
17. 시스템 또는 정보의 무결성	

5. 결 론

본 논문은 국가 주요 기반시설을 대상으로 안전한 클라우드 아키텍처 솔루션를 위해 각 주요국의 클라우드 기술 정책 및 동향·조사에 관한 내용이다. 코로나 19 우리는 클라우드 환경 속에서 다양한 서비스를 제공받고 있으며, 이는 민간분야를 넘어 국가 주요기관 및 공공기관에서 많이 활용되고 있다. 하지만 클라우드를 도입시 발생되는 다양한 보안위협이 존재하기 때문에, 안전한 클라우드 아키텍처 솔루션을 위한 보안기술 적용 및 대응책이 고려되어야 한다.

현재 국내에서 제 3차 클라우드 기본계획을 기반으로, 중앙부처·지차체의 민간클라우드 허용 및 공공·산업 전분야에 클라우드 이용 확산 등 클라우드 대전환을 목표로 추진전략과 과제를 수

행중이며, CSAP를 통해 클라우드의 보안성, 안전성 등을 검토되고 있다.

하지만, CSAP를 미국의 FedRAMP과 비교하였을때, 통제항목이 보안등급에 따라 체계화되어 있지 못하는 단점이 존재한다. 이는 공공기관에서 민간클라우드 도입시 고려해야하는 보안요소이기 때문에, 이에 대한 방안이 제시되지 않으면, 민간클라우드 전환에 있어, 주요국과 비교해 격차가 멀어질 것이다. 국내 클라우드의 발전은 한국판 디지털 뉴딜의 핵심과제인 데이터 댐(데이터 수집, 데이터 축적, 데이터 활용) 등의 구현에 필수적인 인프라 역할을 수행할 것이기 때문에, 이와 관련된 기술, 표준화, 정책, 보안 등 전반적인 요소를 고려하여, 연구 개발 및 투자할 필요가 있다고 사료된다.

본 연구 논문은 한국전자통신연구원 연구운영지원사업의 일환으로 수행되었음 [20ZR1300, TDC 원천기술개발 데이터 커넥팅 기술연구]

참 고 문 헌

[1] 14th IT Strategy Committee. 3rd Cloud Computing Master Plan('22~'24'). (2021). Digital New Deal Korean version of New Deal. https://www.digitalmarket.kr

[2] INNOPOLIS. Promising Market Issue Report Cloud Computing. (2021). Korea Innovation Foundation. https://www.innopolis.or.kr/

[3] NSR. Prospects Report on Future Prospective Information Security Technology for Strengthening National Cybersecurity. (2022). https://www.nst.re.kr/

[4] FSI. Cloud Computing Concepts and Industry Trends. (2016). Security Research Department. https://www.fsec.or.kr/

[5] Y. J. J. et al. Core Infrastructure of Digital New Deal, Cloud Industry Ecosystem Trend. (2021). KDB Future Strategy Research Center Industrial Technology Research Center. https://rd.kdb.co.kr/

[6] W. H. Kang. Cloud Computing Technology Trends. (2018). Science and Technology Job Promotion Agency S&T Market Report, 66. https://www.compa.re.kr/

[7] H. C. Kim, H. K. Lee. et al. AI SW Self-Driving Vehicle Report. (2020). ICT R&D Technical Roadmap 2025. https://www.iitp.kr/

[8] Nipa. Guide to Japanese Cloud Computing Gip Global ICT Portal, 2019. (2019). https://www.nipa.kr/

[9] KOSTEC. 2022 China Cloud Computing White Paper Announced. (2022). Korea-China Science and Technology Cooperation Center. https://kostec.re.kr/

[10] Gartner. Gartner Top 10 Strategic Technology Trends For 2020. (2019). Gartner Information Technology Article. https://www.gartner.com/

[11] IITP. 2018 ICT technology level evaluation results. (2019). https://www.iitp.kr/

[12] S. K. Han. 2021-01 Cloud Service Overseas Trends. (2021). KDI Economic Information Center. https://eiec.kdi.re.kr/

[13] S. K. Han. Cloud Alliance in the EU. (2022). Digital service issue report. https://www.digitalmarket.kr/

[14] C. B. Lee. et al. Cloud Computing Key Statistical Manual. (2017). Ministry of Science and ICT&NIPA. Government of the Republic of Koreanipa. https://www.korea.kr/

[15] Ministry of Public Administration and Security. Administrative/Public Institutions Private Cloud Usage Guidelines. (2019).

Information Resources Policy Division, e-Government Bureau. https://www.korea.kr/
[16] Ministry of Science and ICT & KISA. Cloud Service Security Certification System (IaaS/SaaS/DaaS) Evaluation Criteria. (2020). https://isms.kisa.or.kr/
[17] L. Colonna. Article 4 of the EU Data Protection Directive and the irrelevance of the EU–US Safe Harbor Program?. International Data Privacy Law, 4(3), 203-221.(2014). 10.1093/idpl/ipu005
[18] I. Alsmadi. IT Risk and Security Management. The NICE Cyber Security Framework, 55-78. (2020). 10.1007/978-3-030-41987-5_3
[19] HON Ryan D. McCarthy. The Army Cloud Plan. (2020). https://www.army.mil/
[20] B. H. Lee. et al. Cloud Security Authentication System(FedRAMP) Process Analysis and Government Policy Research. (2013). Korean Standards Association Final Research Report. https://link.springer.com/
[21] IITP. Guidelines for Cloud Usage of Major Information and Communication Infrastructure in the Private Sector. (2021). https://www.iitp.kr/
[22] T. K. Yoon. Cloud Service Security Certification FedRAMP VS CSAP. (2022). Digital service issue report. https://www.digitalmarket.kr/

저 자 소 개

서 대 희(Daehee Seo)

2006.2 순천향대학교 전산학과 박사
2015.3 한국전자통신연구원 선임연구원
2020.5 Kennesaw State University 연구원
2020.9-현재 : 상명대학교 조교수
<주관심분야> 정보보호, 암호 프로토콜, 유무선 네트워크, 클라우드 보안