민간 클라우드 도입 장애요인 분석을 통한 국방 클라우드 도입 전략 도출

박준규* 전우진* 이상훈** 박기웅†

*세종대학교 시스템보안연구실 **국방과학연구소 †세종대학교 정보보호학과

Deployment Strategies of Military Cloud by Analyzing Obstacles to Deployment of Commercialized Cloud Services

Jun-Gyu Park* Woo-Jin Jeon* Sang-Hoon Lee** Ki-Woong Park†

*SysCore Lab., Sejong University

**Agency for Defense Development

† Dept. of computer and information security, Sejong University

요 약

클라우드 컴퓨팅은 인터넷 기술을 활용하여 사용자 요구에 따라 컴퓨팅 자원(네트워크, 서버, 스토리지, S/W)을 서비스로 제공하는 컴퓨팅으로 많은 관심을 받고 있다. 최근 국방 분야에서도 이와 같은 패러다임에 맞춰 클라우드 컴퓨팅 기술에 대한 도입을 추진하고 있다. 기존 연구는 주로 국가 정책이나 공공 기관 중심의 발전 방안을 주로 다루었지만 산업의 근간이 되는 기업 입장에서의 연구는 부족하였다. 따라서 본 논문에서는 국내 기업의 클라우드 도입 장애요인을 서비스 가용성 및 보안 관점에서 분석하여 해당 장애요인을 극복하는 성공적인 국방 클라우드 도입을 위한 전략을 제시하고자 한다.

I. 서론

클라우드 컴퓨팅(Cloud Computing, 이하 '클라우드'로 표기함)은 '인터넷 기술을 활용하여 사용자 요구에 따라 컴퓨팅 자원(네트워크, 서버, 스토리지, S/W)을 서비스로 제공하는 컴퓨팅'이다[1]. 클라우드는 기업 내·외부에 대규모의 IT자원을 확보한 뒤, 인터넷을 통해 접근할 수 있게 하여 규모의 경제를 통해 비용 효율화가 가능하다. 또한, IT자원의 수요가 발생한 시점 혹은 수분 내에 IT자원 확보가 가능하여 클라우드 사용자는 신속한 사업 대응이 가능하게 된다. 다양한 IT자원뿐만 아니라 애플리케이션 및 서비스 등을 통해 기업에게 큰 부담으로 작용하였던 IT에 대한 부담을 축소시켜 기업 및 기관에서는 핵심 사업 및 업무에 대한 집중이 가능하게 되었고, 이러한 이유로 클라우드는 현대 핵심 IT 전략이 되었다.

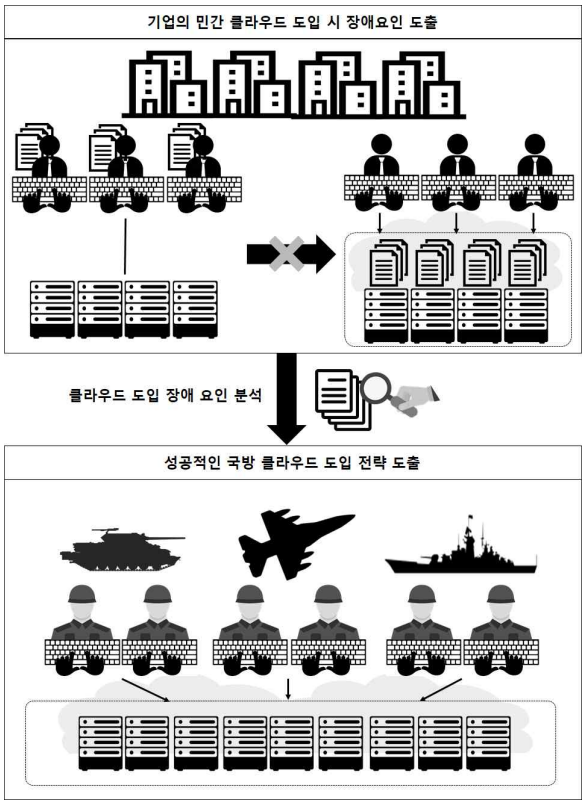
최근 국방 분야에서도 이와 같은 패러다임에 맞춰 클라우드 컴퓨팅 기술에 대한 도입을 추진하고 있다. 안보경영연구원(SMI)에서 2016년에 진행한 '국방 클라우드 컴퓨팅 운영환경 구축방안 연구[2]'를 통해 국방정보자원 운용의 효율화를 위해 클라우드 도입의 필요성을 인식하여 육·해·공군 전산소를 통합한 국방통합데이터센터(DIDC)를 설립하였으며, 전군 공통의 특정 시스템을 대상으로 일부 IaaS(Infrastructure as a Service) 형태의 클라우드 서비스를 제공하고 있는 것을 알 수 있다. 또한, 2013년에 발표한 '국내 클라우드 정책 분석 및 발전방향에 관한 연구[3]'에서는 다양한 프레임워크를 통해 정부의 클라우드 정책을 분석하고, 문제점을 제시하였으며 우리나라의 클라우드 확산 정책이 서비

---

† 교신저자: 박기웅 (세종대학교 정보보호학과 교수)

이 연구는 국방과학연구소의 국방 지휘통제 통합·연동 기반기술 특화연구실 과제의 지원(UD180012ED) 및 2018년도 과학기술정보통신부의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임 (No.2018-0-00420, API 호출 단위 자원 할당 및 사용량 계량이 가능한 서버리스 클라우드 컴퓨팅 기술 개발).

스 소비자가 아닌 서비스 공급자 중심이고, 민간 중심이 아닌 정부 중심이라는 점을 지적하였다. 이를 통해 기존 연구는 주로 국가 정책이나 공공 기관 중심의 발전 방안을 주로 다루었지만 산업의 근간이 되는 기업 입장에서의 연구는 부족한 것을 알 수 있다.



[그림 1] 국방 클라우드 도입 전략 도출 과정

2009년 한국클라우드산업협회(KACI) 민영기의 '클라우드 서비스 활성화를 위한 장애요소 및 대응방안[4]'에서는 클라우드 서비스 활성화 저해요인 중 하나로 클라우드 서비스의 안정성에 대한 우려를 꼽았다. 이는 클라우드를 도입하려는 기업과 국방 분야에 장애요인으로 작용하여 클라우드 도입을 저해하고 있다[5].

클라우드 도입을 저해하는 주요 요인 중 또 다른 하나는 보안이다. 시장조사기관인 IDC가 2016년에 진행한 클라우드 보고서(Cloud Going Mainstream)[6]에는 응답기업의 33%와 1천명 이상 규모의 기업 50%가 보안을 클라우드 도입의 장벽으로 제기하였다. 또한, 2018년 과학기술정보통신부에서 발표한 '2018년 공공부문 클라우드 컴퓨팅 수요조사 결과[7]'에서는 1225개 기관을 대상으로 클라우드 수요조사를 실시하였고, 공공부문의 클라우드 미도입 사유로 보안 우려 및 규제가 24.4%를 기록하였다. 이를 통해 기업 및 공공 분야의 클라우드 도입 장애요인으로 보안에 대한 우려가 존재하는 것을 알 수 있으며, 이는 정보 자원의 중요도가 높은 국방 분야에도 해당 되는 요인이다. 위의 장애요인 외에도 기업의 민간 클라우드 도입 시 발생하는 다양한 장애 요인들이 존재한다.

본 논문에서는 국방 클라우드 도입과 관련성이 높고 기술적으로 해결 가능한 장애 요인들에 대하여 해결 방안을 제시하기 위해 이에 해당하는 장애요인인 서비스 가용성 및 보안 문제를 다룬다. 또한, 정부의 입장이 아닌 클라우드 수요자(사용자) 중심으로 현재 상황을 이해하기 위해 [그림 1]과 같이 국내 기업들의 민간 클라우드 도입을 저해하는 요인을 분석하고, 이를 통해 국방 분야에서 성공적인 클라우드 도입을 위한 방안을 제시하고자 한다.

논문의 구성은 다음과 같다. 2장에서는 국내 기업의 클라우드 도입 장애요인을 서비스 가용성 및 보안 관점에서 분석한다. 3장에서는 분석된 장애요인을 극복하는 성공적인 국방 클라우드 도입을 위한 전략을 제시한다.

II. 기업의 민간 클라우드 도입 시 장애 요인 분석

2.1 서비스 가용성 문제

기업에서 클라우드 도입 후 서비스 장애 발생 시 고객들에 대한 안정적인 서비스 제공 불가능 및 기업 내 업무 처리 지연 등의 문제가 발생한다. 고객들에게 안정적인 서비스를 제공하지 못하는 것은 기업의 신뢰도 및 이익과 직결되는 문제이다. 이에 따라 기업에서는 기존 시스템에서 클라우드로 전환 후 발생할 수 있는 서비스 장애에 대한 우려로 인해 클라우드를 도입하지 않는 결론에 도달하게 된다.

2.2 보안에 대한 우려

클라우드에서 가상화 기술과 하나의 소프트웨어를 여러 테넌트(사용자)가 공유해서 사용할 수 있도록 하는 멀티테넌시 기술은 핵심 기술이다. 하지만, 이러한 기술을 사용함으로 인하

여 인증 및 접근제어의 복잡도가 상승한다. 이에 따른 관리 부주의 및 설정 오류 등으로 클라우드 이용자의 정보가 유출되는 문제가 발생할 수 있고, 이는 클라우드 보안의 핵심 이슈이다[8]. 특히, 기업에서 경영정보 및 개인정보와 같은 민감한 정보들이 잘못 관리되어 보안 사고가 발생하면 기업에게는 큰 타격이 발생한다.

III. 성공적인 국방 클라우드 도입 전략

UC 버클리대학교에서 연구한 '09년 클라우드 컴퓨팅 확산 시 예측되는 10가지 장애요인과 해결방안[9]' 결과 중 서비스 가용성에 해당하는 해결방안과 2017년 소프트웨어정책연구소(SPRi)에서 발표한 '클라우드 보안의 핵심이슈와 대응책[8]'에서의 보안 문제 해결방안은 아래 표 1에 나타나있다. 하지만, 민간과 국방의 상이한 특성으로 인해 민간에서의 해결방안을 국방에 완벽히 적용시키는 것은 불가능하다. 따라서 본 장에서는 민간에서의 해결방안을 토대로 성공적인 국방 클라우드 도입 전략을 제시한다.

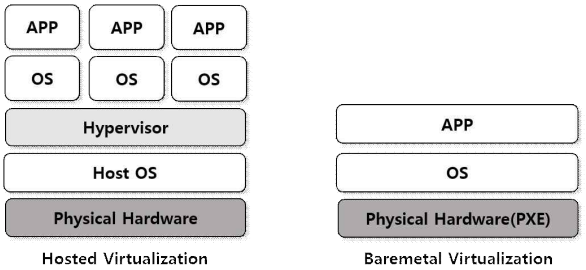
장애요인	민간에서의 해결방안	국방에서의 해결방안
서비스 가용성	다수의 클라우드 공급자 활용	- 베어메탈 방식을 이용한 하이브리드 클라우드 도입
보안에 대한 우려	기존의 보안 방식의 재구성을 통한 방어체계 구축	

[표 1] 클라우드 컴퓨팅 확산 시 기술적 장애요인과 민간 및 국방에서의 해결방안

3.1 베어메탈 방식을 이용한 하이브리드 클라우드 도입

본 논문에서의 하이브리드 클라우드(Hybrid Cloud)란 [그림 2]와 같이 하드웨어의 리소스를 공유하는 호스트 기반 가상화 방식과 리소스를 공유하지 않는 격리된 환경에서의 단독 인프라가 제공되는 베어메탈 방식을 혼용하여 구성하는 클라우드 방식이다.

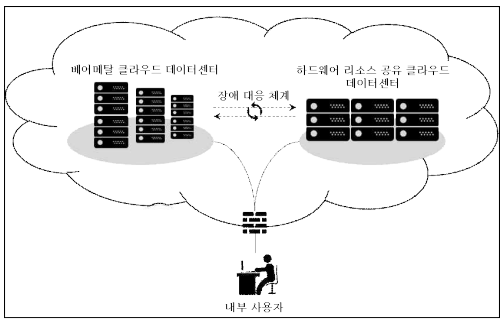
베어메탈이란 PXE(Preboot Execution Environment)를 활용하여 네트워크로 운영체제를 부팅할 수 있게 해주는 환경이다. PXE란 BIOS 및 NIC(Network Interface Card)를 통해 디스크 대신 네트워크에서 컴퓨터를 부트스트랩을 할 수 있도록 해주는 기술이다. 네트워크를 통해 시스템을 부팅 할 수 있는 기능을 사용하여 서버를 배포 및 관리한다. 또한, 사용자에게는 하드웨어의 리소스를 공유하지 않는 격리된 환경에서의 단독 인프라가 제공된다. 이러한 베어메탈 방식을 활용한 하이브리드 클라우드를 이용할 경우, 클라우드 도입을 저해하는 요인인 서비스 가용성과 보안에 대한 우려를 해결하는 것이 가능하다.



[그림 2] 호스트 기반 가상화 방식과 베어메탈 방식

3.1.1 물리적으로 구분된 특성으로 서비스 가용성 문제 해결

'K-ICT 클라우드 컴퓨팅 활성화 계획[10]'에 따르면 중앙행정기관, 지자체, 공공기관 대부분 정보 자원의 중요도가 높으므로 민간 클라우드보다 정부 클라우드 및 자체 클라우드를 이용하도록 하고 있다. 이로 인해 높은 중요도를 가지고 있는 군의 정보자원 특성상 자체 클라우드를 구축하여야만 한다. 통합데이터센터를 구축하여 자체 클라우드를 이용할 경우, 서비스 장애 발생 시 집중화된 시스템으로 인해 모든 시스템이 마비될 가능성이 존재한다. 하지만, 하이브리드 클라우드를 도입할 경우 [그림 3]과 같이 데이터센터 간 물리적으로 분리된 특성으로 인해 서비스 장애 발생 시 가용성 확보가 가능한 이점이 있다. 물론, 서로 다른 위치의 데이터센터 간 장애 대응 체계가 구축되어 있어야한다.



[그림 3] 하이브리드 클라우드 구성도

3.1.2 격리된 환경으로 보안에 대한 우려 감소

베어메탈 방식을 이용할 경우 격리된 환경에서의 단독 인프라가 제공되기에 하드웨어 리소스를 공유하지 않으므로 정보가 유출될 가능성이 낮다. 가령, 군에서 호스트 기반 가상화 방식을 이용할 경우 각기 다른 성격을 가진 기관의 유출되어서는 안 될 정보가 관리 부주의 및 설정 오류 등으로 유출될 가능성이 있다. 하지만, 군의 정보자원 중 더욱 높은 중요도를 가진 정보자원과 관련된 군 내부 기관 및 업무 수행의 경우 베어메탈 방식을 이용하여 타 기관 및 업무와의 격리를 통해 정보 유출 가능성을 낮추어 보안에 대한 우려를 감소시키는 것이 가능하다.

IV. 결론

본 논문에서는 국내 기업 관점에서 민간 클라우드 도입을 저해하는 요인을 분석하고 이를 통해 성공적으로 국방 분야에 클라우드를 도입하기 위한 전략을 제안하였다.

우리나라는 클라우드 산업이 활성화 되기 위한 우수한 ICT 인프라를 보유하고 있으며, 정부의 관련 법과 제도 제정으로 지속적으로 클라우드 산업 규모가 성장하고 있다. 하지만, 클라우드 도입을 저해하는 서비스 가용성 문제 및 클라우드 보안에 대한 우려가 존재하고 있다. 이와 같은 문제를 해결하기 위해 본 논문에서는 국내 기업 관점에서 민간 클라우드 도입을 저해하는 요인을 분석하고 이를 통해 성공적인 국방 클라우드 도입 전략으로 베어메탈 방식을 이용한 하이브리드 클라우드를 도입하여 서비스 가용성 문제와 보안에 대한 우려를 감소시키도록 제안하였다.

추후 연구에서는 더욱 다양한 측면에서 클라우드 도입 장애 요인을 분석하여 성공적으로 국방 분야에 클라우드를 도입하기 위한 전략에 대한 연구를 수행할 것이다.

[참고문헌]

[1] P.MELL, T.Grance. “The NIST definition of cloud computing”, 2011.

[2] 안보경영연구원(SMI), “국방 클라우드컴퓨팅 운영환경 구축방안 연구”, 2016.

[3] 백승익, 신지연, 김종우, “국내 클라우드 정책 분석 및 발전방향에 관한 연구”, 한국전자거래학회지 제18권 제3호, 2013.

[4] 민영기, “클라우드 서비스 활성화를 위한 장애요소 및 대응방안”, 한국정보통신기술협회 저널 125호, 2009.

[5] 김성태, “클라우드 컴퓨팅의 동향과 군 도입 시 고려사항(1)”, 한국국방연구원 주간국방논단 통권 제1386호, 2011.

[6] IDC(International Data Corporation), “Cloud Going Mainstream: All Are Trying, Some Are Benefiting; Few Are Maximizing Value”, 2016.

[7] 과학기술정보통신부, 행정안전부, “2018 공공부문 클라우드 컴퓨팅 수요조사 결과”, 2018.

[8] 정성재, 배유미. "클라우드 보안 위협요소와 기술 동향 분석" 보안공학연구논문지 10.2 , 2013.

[9] M. Armbrust and Armando Fox, and et al., "Above the Clouds: A Berkeley View of Cloud Computing," EECS Department, University of California, Berkeley Technical Report, No.UCB/EECS-2009-28, 2009.

[10] 미래창조과학부, “K-ICT 클라우드 컴퓨팅 활성화 계획”, 2017.