Regular paper | Journal of the KIECS. pp. 687-694, vol. 15, no. 4, Aug. 31. 2020, t. 102, pISSN 1975-8170 | eISSN 2288-2189
http://dx.doi.org/10.13067/JKIECS.2020.15.4.687

SDN/NFV의 군 적용 타당성 분석

장지희* · 권태욱**

The Validity Analysis of SDN/NFV Military application

Ji-Hee Jang* · Tae-Uk Kwon**

요 약

SDN과 NFV은 차세대 네트워크 기술로서, 데이터센터, 캠퍼스, 대형회사 등 Cloud가 구축되어 있거나, 서비스 제공 중심의 통신회사 등에서 활발하게 적용하고 있다. 특히, 軍 적용을 위해서는 국방통합데이터센터가 대표적인 예가 될 것이다. 국방통합데이터센터(DIDC)가 지능화된 센터로 도약하기 위해 최신 정보통신기술(ICT)을 적용한 「스마트 국방통합데이터센터」 추진에 박차를 가하고 있다. DIDC 설립 당시, Cloud 서비스 등의 인프라 구축을 30% 안팎의 수준으로 시작하여, 현재 'Cloud 퍼스트'를 통해 D-Cloud를 75%까지 확장할 예정이다. 또한, SDN/NFV 도입하므로 DIDC의 운용비용과 인력을 절감하고, 정보자원의 효율적인 이용과 사이버 정보보호체계에 대한 능력을 강화할 예정이며, 각 체계 사용에 유연성과 민첩성을 높여 앞으로 국방경영에 효율성에 이바지하기 위해 노력하고 있다. 이에 DIDC을 중심으로 SDN/NFV 도입의 당위성과 기대효과를 논하고자 한다.

ABSTRACT

SDN and NFV are next-generation network technologies, and cloud, such as data centers, campuses, and large companies, has been established, or is actively applied by service-oriented communication companies. In particular, the Defense Integrated Data Center will be a prime example for military applications. In order for the Defense Integrated Data Center (DIDC) to become an intelligent center, it is accelerating the promotion of the "Smart Defense Integrated Data Center", which applied the latest information and communication technology (ICT). At the time of the establishment of DIDC, it plans to start building infrastructure such as cloud services at around 30% level, and expand D-Cloud to 75% through 'Cloud First'. In addition, the introduction of SDN/NFV will reduce the operation cost and manpower of DIDC, strengthen the ability to efficiently use information resources and cyber information protection systems, and increase flexibility and agility in using each system to improve efficiency in defense management in the future. Therefore, we will discuss the justification and expected effects of SDN/NFV introduction, focusing on DIDC.

키워드

Data Center, SDN, NFV, Cloud, Next generation Networking
데이터센터, SDN, NFV, Cloud, 차세대 네트워킹

* 국방대학교 석사과정(sunrain8659@korea.kr)
** 교신저자 : 국방대학교 컴퓨터공학과 교수
· 접 수 일 : 2020. 06. 25
· 수정완료일 : 2020. 07. 20
· 게재확정일 : 2020. 08. 15
· Received : Jun. 25, 2020, Revised : Jul. 20, 2020, Accepted : Aug. 15, 2020
· Corresponding Author : Tae-Uk Kwon
Dept. Computer Science, Korea National Defense University,
Email : sunrain8659@korea.kr, kwontw9042@kndu.ac.kr

Ⅰ. 서 론

일반 데이터센터에 SDN(:Software Defined Networking)과 NFV(:Network Function Virtualization)를 도입한다는 것은 별반 새롭지 않은 사실이겠지만, 국방통합데이터센터(Defense Integrated Data Center, DIDC)의 경우, SDN 도입공사 소식은 다른 데이터센터보다 의미 있는 행보이다.

DIDC는 창군 이래 최대 규모의 국방 정보화 사업으로 꼽히며, 전국에 흩어져 있던 육·해·공군의 240개소의 1,100여 개의 국방정보시스템을 통합 운영하기 위해 설립하였다[1]. 하지만 대규모 통합을 위해 설립된 DIDC의 인력은 각 군으로부터 단시간에 전환 편성되었으며, 이에 적용된 인사정책 역시 각 부대의 책임 하에 분리되어 이루어졌다. 이렇게 편성된 인원은 당시 각 군의 컴퓨터 체계에 대한 업무 지식과 경험이 부족한 상태로 다수·다종의 서버, 스토리지, 네트워크 장비 등을 관리·운용해야 했다[2].

당시 정부 3.0 발전계획 중 「Cloud 컴퓨팅 기반의 지능정부 구현」 과제에 따라, 공공부문의 선도 하에 Cloud 컴퓨팅을 활성화하기 위한 정책으로 데이터센터 설립을 위해 일부 시스템을 대상으로 IaaS(:Infrastructure as a Service) 형태[3]의 Cloud 서비스를 제공하였지만, 이러한 첨단 인프라는 인력 부족, 이기종의 복잡한 네트워크 구조 및 1,600개의 정보시스템을 관리·운용으로 인하여 지금까지 많은 어려움과 제한사항이 있었을 것으로 예상한다.

또한, Cloud 서비스 등 최첨단 인프라의 구축은 여전히 30% 안팎 수준이기 때문에, 4차 산업혁명으로의 정보통신기술(ICT)을 적용한 “스마트 DIDC”로의 추진을 위해서 더욱 박차를 가해야 할 것이다.

본 고에서는 국방대학교에서 지속해서 연구되었던 주제인 DIDC의 SDN/NFV 적용 방안에 대하여 다시 한번 검증의 시간을 갖고, DIDC의 Legacy 체계와 SDN/NFV 체계를 비교 실험하여, 그에 따른 기대효과와 당위성에 대하여 논하고자 한다.

Ⅱ. 본 론

2.1 D-Cloud로 전환

국방개혁 기본계획에 따라 국방정보 시스템 중 컴퓨터 체계를 통합 관리·운용하기 위해, 군 장비의 효과적인 운용을 위해 DIDC는 각지에 산재하여 있던 육·해·공군 전산소의 정보시스템들을 과감히 청산하여 통합하면서 국방 정보화 핵심 센터가 되었다.

그에 따라, 국방부는 2019년 ‘Cloud 퍼스트’ 정책을 추진함에 따라 DIDC의 신규 시스템 구축 또는 노후 시스템 교체 시 Cloud로 전환될 예정이다. 이는 DIDC의 Cloud 내 공간을 ‘D-Cloud’로 전환하여 정보자원 활용을 높이고, 예산 절감 효과를 기대할 수 있게 되었다. 그리고 Cloud에 인공지능(AI), 빅데이터 등을 접목하여 장애 예측과 침해 예방 시스템 구축이 가능해졌다.

데이터센터를 설립할 당시, 과거부터 각 군의 체계에 맞게 운영되던 정보통신 장비(네트워크 장비와 서버, 스토리지)들을 물리적으로 이동시켜 운영하다 보니 각기 다른 서버운영체제 및 설계된 프로토콜과 유지관리 비용 등은 지속해서 문제점으로 도출되었다. 이러한 문제를 해결하기 위해서 Cloud 전환은 더욱 필요한 사업이었다.

그러므로 DIDC는 안정적인 Cloud 도입을 위해 각 일정 기간을 두고, 점차 전환율을 높여갈 예정이다. 표1은 3단계로 나누어 Cloud 전환을 보여준다[1].

표 1. Cloud 전환 3단계

Table 1. Cloud transition 3 stages

stage	period(year)	transformation Ratio	Description
1	2019~2020	40%	Cloud activation
2	2021~2022	60%	Cloud maturization
3	2023~	75%	Cloud intellectualization

특히, 데이터센터에 도입될 프라이빗 Cloud 방식은 데이터센터를 중심으로 Cloud 컴퓨팅 환경을 구성하여 내부 고객에게만 서비스를 제공하는 방식으로 공통된 업무 관심을 가진 군의 특성을 만족시키는 동시에 오케스트레이션(orchestration)과 자동화를 지원하는 가상화 컴퓨팅, 네트워크, 그리고 스토리지 리소스(resource) 등을 위해 구성되므로, 실행 시 해당 사용자의 방화벽으로 보호할 수 있어 특정한 보안 측면 요구사항이나 효과에 우수하다고 알려져 있다[4]. 또

한, 이를 구축하기 위한 컨설팅, 구축, 하드웨어, 솔루션(가상화, 네트워크 등)에 대한 수요는 오픈소스와 국산 소프트웨어 도입을 통해 비용 절감뿐만 아니라 정보자원운영 효율성 측면에서 데이터센터의 신속한 대응과 안정적인 서비스까지도 달성할 것으로 예상할 수 있다.

2.2 DIDC의 SDN 도입

데이터센터의 D-Cloud의 전환에 따라, DIDC의 네트워크 구조는 기본적으로 scale-out 환경으로 조성될 것이며, 그에 맞는 유연한 구조가 구축되어야 할 것이다. 기존 DIDC 내 네트워크 장비는 벤더(vendor)별 서로 다른 폐쇄적인 운영체제를 가지고 있어, 호환성이 부족하고 센터의 환경에 맞는 혁신적인 네트워크 서비스 구현이 불가하였다.

이러한 요구사항들은 Cloud 환경의 확산에 따라 필연적인 요소로 자리 잡아가고 있으며, 서버, 스토리지뿐 아니라 네트워크 관점에서 Cloud 서비스 환경에 적합한 혁신적인 기술의 네트워크 아키텍처가 필요하게 되었다[5].

SDN은 소프트웨어 정의 네트워크로서, 개방형 API(오픈플로우)를 통해 네트워크의 트래픽 전달 동작을 소프트웨어 기반 컨트롤러에서 제어/관리하는 접근 방식이다[5].

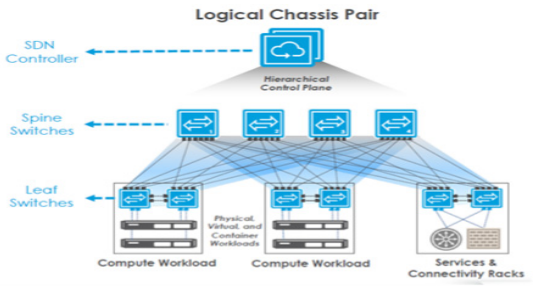

그림 1. SDN 계층구조[6]

Fig. 1 SDN hierarchy

SDN은 네트워크 장비에서 H/W와 S/W 기능을 분리하는 것이 핵심인데, 먼저, H/W 영역은 Data Plane으로 데이터를 전송하는 역할을 담당한다. 그리고 S/W 영역은 Control Plane과 Application Plane으로 나뉘며, Control Plane은 네트워크에 대한 정책을 적용하는 역할을 담당하고, Application Plane은 정책 적용을 위한 사용자 지원 역할을 한다.

결국, Control Plane은 SDN Controller로 구현되어, 논리적으로 중앙 집중화하도록 프로그래밍되어, 네트워크의 제어나 흐름, 혼잡 제어 등에 유연성을 제공하게 된다.

그림 1과 같이 SDN이 데이터센터에 도입된다면, 각 서버와 스토리지와 연결된 스위치와 이러한 스위치를 연결한 중간 스위치, 그리고 이들을 통제하는 SDN Controller가 위치할 것이다.

이러한 SDN은 물리적 스위치 영역에 효율적인 네트워크 관리 및 지능화 단계로 이르게 하여, 네트워크 환경의 효율적인 아키텍처로 DIDC에 꼭 필요한 요소가 될 것이다.

게다가 육군 자체만 하더라도 000개에 달하는 자체 개발 SW는 단순한 접속만 제공하였던 기존의 인프라에서 벗어나 현재 육군에서 개발 중이거나, 투자되고 있는 드론, 인공지능, 빅데이터, 사이버방호, VR 등 다양한 디바이스 및 광대역 유무선 접속을 위한 자원 및 기능 가상화, 응용 기반의 네트워킹과 컴퓨팅 자원 제어 및 관리, 서비스-ICT 자원 조율이 가능하게 할 것이며, 이기종의 장비를 수용할 수 있는 인프라의 확장성과 유연성을 갖춘 SDN 네트워크 기술을 통해 스마트 DIDC를 구축할 수 있을 것이다.

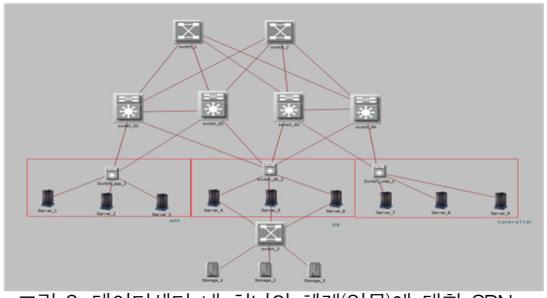

그림 2. 데이터센터 내 하나의 체계(업무)에 대한 SDN 구성(예)

Fig. 2 SDN configuration for one system(task) in DIDC(example)

그림 2와 같이 데이터센터에 SDN 구성하고 있는 여러 시스템 중 하나를 예로 들었을 때, 각각의 APP, DB, WEB 서버 등에 연결된 Data Plane 스위치를 상위에 있는 Control Plane이 통제하여, Legacy 체계와

같이 네트워크 장비업체의 프로토콜과 운영체제에 종속되지 않고, 데이터센터 자체적인 중앙집중적 관리를 통해, SDN 계층 사이에 인터페이스의 결합 없이 단순화된 서비스를 제공할 수 있을 것이다.

전체적인 관점에서 소프트웨어 정의에 기반한 통제 및 관리는 DIDC의 민첩성과 유연성을 높여줄 수 있으며, 상세한 네트워크 분석이 가능하여 유사시 국방통합데이터센터에 맞는 대응과 조치를 할 수 있을 것으로 예상한다.

2.3 네트워크 장비에서의 NFV의 도입

NFV는 IT 가상화 기술을 사용하여 전체 클래스의 네트워크 노드 기능을 연결 또는 구조화하여 통신 서비스를 생성할 수 있는 블록으로 가상화하는 네트워크 아키텍처 개념이다.

이러한 NFV가 SDN을 반드시 통하여 구현되는 것은 아니지만, NFV를 SDN 소프트웨어에 탑재하여 구동하였을 때, 인프라를 공유할 수 있고, 필요한 기능 적용과 관리 효율성 증대에 따라 SDN 환경에서 NFV 구현에 대한 이점이 많다.

DIDC 설립 당시, 전국의 전산소 장비의 통합·운영을 위해 각 장비의 물리적 이동을 하였으며, 각기 다른 네트워크 장비 운용에 어려움이 있었다. 하지만 SDN 도입을 통해 스위치에 대한 중앙집중 관리·운영이 가능해졌다 하더라도, 데이터센터에는 스위치 외에 여러 네트워크 장비의 통합이 필요하다.

이러한 여러 네트워크 기능을 NFV로 가상화하게 되면, 많은 제약 사항들을 대부분 해결할 뿐 아니라 SDN 구축에 따른 추가적인 혜택을 가져올 수 있을 것이라 예상한다.

DIDC의 Legacy 네트워크 체계는 각종 서버에 대한 원활한 통제 및 성능 보장을 주목적으로 한다.

표 2. 각 장비별 중복 기능 비율
Table 2. Percentage of overlapped functions for each device

	L4	TAP	QoS	DPI	avg.
overlapped functions	31	10	17	20	20
Ratio(%)	67.3	100	50	60.6	69.5

TCP/IP 계층에 속하는 IP 및 Port 정보 등을 통해 스위칭 및 로드밸런싱을 지원하는 L4 스위치, 각 노드 간의 트래픽을 모니터링하는 TAP, 데이터 서비스에 대한 성능을 보장하는 QoS, 패킷에 대한 심층 분석을 통하여 트래픽을 관리하는 DPI, 총 4개의 장비를 대상으로 NFV로 통합하고자 한다. 선정된 장비의 기능은 벤더별 상이할 수 있어, 최대한 많은 기능을 포함한 장비를 두 개 이상 선정하여 수행하였다.

위의 4가지의 장비들을 L3, Management, High Availability의 총 3개 그룹으로 나누어 각 장비가 보편적으로 보유한 52개의 기능을 분석한 결과, 체계별로 고유기능을 제외하고 평균 69.5%의 기능이 중복요소를 보유함에 따라, 이를 통합하여 중복수행을 감소시켜, 더욱 효율적인 네트워크 체계를 구현할 수 있다고 예상하였다[6].

2.4 정보보호 장비에서의 NFV의 도입

데이터센터에는 효율적인 네트워킹 이슈뿐 아니라 가장 중요시되는 이슈가 있다. DIDC는 특수한 목적으로 설립되었기 때문에, 해킹의 위협으로부터 비밀유출방지를 위해, 보안 관점에서 내부자원의 유출방지 솔루션 구축에 큰 비용과 시간을 투자하고 있다. 특히 사이버 위협으로부터 센터는 국방 핵심 정보자산을 방호하기 위해 영역별·기능별 다단계 방어체계를 구축해 방화벽 등 25종 314대의 정보보호체계를 운용하고 있다[8].

이러한 정보자산은 센터 안의 네트워크 구조와 센터 밖에서 처리되는 트래픽에 영향을 미칠 수밖에 없다. 이러한 이유로 많은 군 관계자라면 느린 네트워크 속도에 민감하다.

그러므로 DIDC가 SDN 네트워크 기반으로 구축이 완료되었을 때, Legacy 네트워크 정보보호체계를 대체할 수 있는 NFV 기술을 활용한 네트워크 정보보호 체계 설계를 통하여 트래픽 속도를 개선하고, 프로세스 간 처리결과 공유와 프로세스 중복실행 최소화를 보다 효율적으로 보안 목표를 달성할 수 있는 체계구현이 가능하도록 하겠다.

특히 정보보호 모니터링 시 대표적으로 활용되는 네 개의 장비의 기능을 살펴보았다.

침입 차단 시스템(Fire Wall)과 침입 방지 시스템(Intrusion Prevention, IPS), 그리고 보안 목적상 분산

서비스 거부공격(Distributed Denial of Service, DDoS)을 탐지 및 차단할 수 있는 Anti DDoS 체계가 그것인데, 이 장비들을 대상으로 공통적으로 실행되는 프로세스를 NFV기술로 통합하여 성능향상, 관리의 효율성과 유지보수의 용이성이라는 이점을 달성하고자 한다.

네트워크 정보보호체계들은 크게 5가지 보안 기능 요구사항(Security Functional requirements, SFR) Class를 공통적으로 보유하면서, 체계별로 목적에 따라 추가적인 기능을 보유한다. 공통적인 기능은 보안감사, 사용자 데이터 보호, 식별 및 인증, 보안관리, TSF(TOE(Target of Evaluation) Security Functionality) 보호가 그것인데, 통합 운영이 필요하거나 유리하다고 판단된 41개, 즉, DIDC와 유사한 구조의 네트워크 정보보호체계를 운영한 공군부대의 장비를 대상으로 선정하여 보편적으로 가지고 있는 보유기능을 기준으로 단순히 정량적으로 계산해 보면, 각 정보보호체계의 고유기능을 제외하고 대다수 기능과 프로세스가 중복이 평균 56%가 된다는 사실을 표 3과 같이 알 수 있었다[9].

표 3. 각 정보보호 장비의 체계별 SFR 중복 비율
Table 3. Percentage of SFR overlapped functions by system of each information protection equipment

	Firewall	IPS	Anti DDoS	avg.
overlapped functions	21	24	24	23
Ratio(%)	51	58.5	58.5	56.1

그러므로 정보보호 장비의 중복된 기능과 고유기능을 NFV를 통해 가상화하여 SDN 스위치와 동작하게 한다면 안전하고 단순한 네트워크 아키텍처를 달성할 수 있을 것이다.

하지만 앞서 주의해야 할 사항은 5가지 주요 SFR Class가 Firewall과 IPS, 비정상 트래픽 탐지/차단체계에 모두 동일하게 식별되지만, 이 모든 장비가 다르게 설계된 것이므로 같이 볼 수 없다. 역할과 처리방식에 따라, 서로 다른 감사 대상(IP, Port / 패킷 헤더, 트래픽량 등)으로 세부적으로는 서로 다름을 고려하여 설계해야 하겠다.

2.5 실험 결과 및 기대 효과

시뮬레이션은 상용 SW인 'Riverbed Modeler'를 사용하여, 데이터센터의 Legacy 네트워크 구조, SDN 구조, NFV 구조를 구상하여 이를 비교하였으며, 대상은 데이터센터 내 가장 많이 사용하는 5가지 주요 체계(이메일, 홈페이지, 행정업무 등)로 하였으며, 센터와 같게 설계하기 위해 노력하였다.

그 결과, 먼저, Legacy 네트워크 구조와 SDN 구조를 비교하여 트래픽의 차이가 없었으나, 자연재해 또는 장비 고장으로 인한 네트워크 단절 상황 발생 시 이를 대체하거나, 대안을 찾는 복구 시간에 대한 차이가 발생할 것으로 예상한다.

또한, 2017년 과기정통부 연구에 따르면, Legacy 체계와 SDN/NFV 통합 관리를 위한 메커니즘을 지속해서 연구하여, 이전 기술의 통합 관리 시스템 및 통합 관리에 따른 장애 관리 알고리즘 연구 개발을 위해 노력하고 있음을 알 수 있었다[10].

그러므로 데이터센터의 모든 장비에 대해 SDN을 도입하지 않더라도 D-Cloud가 적용될 군 업무체계에 대한 네트워크 건축을 대상으로 구 체계와 신 체계의 통합·관리가 가능하겠다.

두 번째로, 네트워크 장비 및 정보보호체계를 SDN 및 NFV로 가상화한 네트워크 아키텍처를 Legacy 체계와 비교하였다.

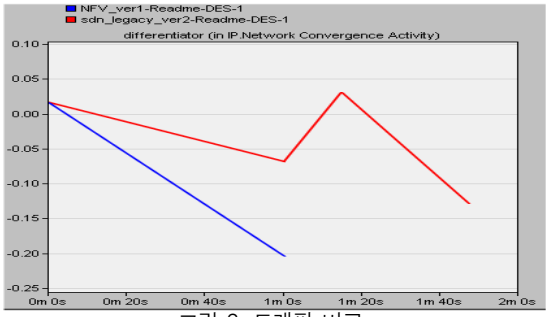

그림 3. 트래픽 비교
Fig. 3 Traffic comparison

그 결과, 그림 3과 같이 네트워크 트래픽 관련하여 Legacy의 트래픽 측정은 1m 50s인 데 비해, SDN/NFV 체계는 1m 0s가 소요되는 것을 확인하였으며, 이는 트래픽 속도 측면에서 54% 개선된 것을

알 수 있는데, 전반적인 군 네트워크 개선을 가져올 수도 있을 것이라 예상한다.

결과적으로 SDN/NFV를 통해 데이터센터 내 주요 장비에 대한 중복기능 최소화를 통해 효율성 향상 및 전력 낭비 최소화와 지금까지 문제가 되었던 스위치에 대한 벤더 종속성 탈피를 통해 유연성 체계 업데이트 및 확장 가능, 가상화 기능을 이용한 간단없는 통신망 가동상태 유지라는 이점을 기대하므로, 장기적으로 비용 절감이라는 효과도 얻을 수 있을 것이다.

특히 정보보호체계의 통합을 NFV로 달성하게 된다면, 정보보호 기능의 가상화 및 컴포넌트화되어 각 서버에서 동작이 효율적이며, 논리적 다중화를 통해 유사시 체계 생존성을 높일 수 있을 것이라 예상된다. 그러므로 현재까지 도출되었던 DIDC의 당면 과제를 해결하고, 지능화된 Cloud 확장이 가능하겠다.

III. 결론 및 향후 연구

이제 D-Cloud가 없는 DIDC를 상상하기는 힘들 것이다. 현재 군은 AI(인공지능), 드론, VR/AR 관련 국방적용을 위해 연구 또는 사업을 집행하고 있다. 그에 따라 데이터센터는 유·무선 및 그 스펙트럼을 수용해야 하며, 새로운 장비에 대한 보안정책 또한, 매우 중요한 사안이라고 생각한다.

그렇다면 데이터센터가 어떠한 네트워크 형식의 아키텍처로 갈 것인지 신중하게 생각해야 할 것이다.

현재, 이기종 서버 및 네트워크 장비에 따른 관리 및 운용의 문제로 인하여, 첨단 국방통합데이터센터로 어려움에 부닥쳐 있었을 것이다.

이제 DIDC는 'Cloud 퍼스트 정책' 추진과 맞물려 SDN/NFV의 도입을 통해, 4차 산업혁명 핵심기술을 선도하는 부대로서 면모를 갖출 것으로 예상한다.

향후 연구로, DIDC에 적합한 Legacy 체계와 SDN 체계의 통합 수준을 확인하고, 그에 따라 SDN/NFV를 통해 장애 발생 여부 예측 및 해결에 대한 방안에 대하여 연구하도록 하겠다.

지금까지는 수많은 장비가 복잡하게 얽힌 모습이었다면, D-Cloud 시스템과 Cloud 지능화를 위한 SDN/NFV 도입으로 다양한 수요를 충족시키기 위해 유연성과 확장성을 두루 갖춘 「스마트 DIDC」로 전진할 것이다.

References

[1] J. Kim, "The Ministry of National Defense is promoting 'Cloud First' policy, Within three years, more than 60% of the systems will be in the cloud," *Electronic News, J,* June. 2019

[2] Y. Park, "A study on competency evaluation model for strengthening DIDC professional manpower," *J. of Dodo IT, July* 2018, pp. 01-35.

[3] S. Lee, "The Study on Development of Technology for Electronic Government of S. Korea with Cloud Computing analysed by the Application of Scenario Planning," *J. of the Korea Institute of Electronic Communication Sciences,* June 2016, vol 7, no. 06 pp. 1245-1258.

[4] K. Choi, "Strategies for applying private cloud computing", J of National IT Promotion Agency, June 2011, pp. 01-11.

[5] M. Lee, "Implementation of a Platform for the Big Scientific Data Transfers," *J. of the Korea Institute of Electronic Communication Sciences,* Aug 2018, vol 13, no. 04 pp. 881-886.

[6] "SDN Education material" In *Proc. Naim Co*

[7] W, Chae, "A Study on the Design of Network Architecture for DIDC Using NFV", In *Proc. Korea National Defense University,* 2019, pp. 36-48.

[8] H, Woo, "Efficient Defense Management Efficiency with the Defense Integrated Data Center 'Smart Defense Integrated Data Center'" J of Kukbangilbo, July 2019

[9] Kang, "A study on the Design of Network Security System for DIDC Using SDN/NFV," In *Proc. Korea National Defense University,* 2017, pp. 47-51.

[10] T, Kwon, "Next-generation network environment(SDN) and legacy network environment Development of support-oriented network management system", In *Proc. Ministry of Science and ICT,* 2017, pp. 08-59.

저자 소개

장지희(Ji-Hee Jang)

2009년 경남대학교 군사학과 졸업 (학사)
2019년 ~ 현재 국방대학교 대학원 컴퓨터공학과 석사과정
※ 관심분야 : 네트워크, SDN, NFV, 데이터센터

권태욱(Tae-Wook Kwon)

1986년 육군사관학교 컴퓨터공학과 졸업(공학사)
1995 미국 해군대학원 컴퓨터공학 (공학석사)
2001년 연세대학교 컴퓨터공학과(공학박사)
2007년 ~ 현재 국방대학교 컴퓨터공학과 교수
※ 관심분야 : 네트워크, Sensor Networking, CCN, SDN, NFV