논문 19-45-02-24 The Journal of Korean Institute of Communications and Information Sciences '20-02 Vol.45 No.02
https://doi.org/10.7840/kics.2020.45.2.400

클라우드 기반 미래 한국군 지휘통제체계 보안 아키텍처 설계

구 자 훈◆, 김 영 갑°, 이 상 훈*

Design of Security Architecture for the Cloud-Based Korea Military Command and Control System

Jahoon Koo◆, Young-Gab Kim°, Sang Hoon Lee*

요 약

최근 클라우드 컴퓨팅 기술의 발전과 함께 미국과 같은 선진국들은 클라우드 도입 정책들을 통해 국방 및 공공 부문 효율화, 국가혁신 추진, 클라우드 컴퓨팅 이용 환경 개선을 위한 인프라 구축 등을 추진 중이다. 한국도 클라우드법을 제정하고 여러 분야에서의 클라우드 도입을 고려중이다. 특히 국방 분야에서도 지휘통제체계에 클라우드 적용을 고려중이며 관련 연구수행과 시범 사업을 진행하고 있다. 그러나 현 한국군 정보시스템이 클라우드 컴퓨팅 시스템으로 전환되었을 경우, 기존의 보안 요구사항만으로는 클라우드 컴퓨팅 관련 보안 취약점을 해결할 수 없다. 즉, 클라우드 기반의 안전한 지휘통제체계 시스템을 구축하기 위해서는 기존 보안 요구사항에 부족한 클라우드 컴퓨팅 관련 보안 요구사항을 추가로 도출할 필요가 있으며, 이를 기반으로 보안 아키텍처 설계가 필요하다. 본 논문에서는 클라우드 기반 지휘통제체계가 갖추어야 할 보안 요구사항을 도출하고 이를 기반으로 설계된 보안 아키텍처를 제안한다.

키워드 : 지휘통제체계, C4I, 국방 클라우드 보안 요구사항, 국방 클라우드 보안아키텍처, 접근통제
Key Words : Command and Control System, C4I, Security Requirements for National Defense Cloud, Security Architecture for National Defense Cloud, Access Control

ABSTRACT

With the development of cloud computing technology, developed countries including the U.S. are performing the efficiency of national defense and public sector, national innovation, and construction of the infrastructure for cloud computing environment through the policies that apply cloud computing. Republic of Korea is also enacting the cloud act and considering cloud adoption in various fields. In particular, it is considering the applying the cloud to the command control system in the national defense sector, and is conducting related research and pilot projects. However, if the existing korea information system is converted to a cloud computing system, only existing security requirements cannot solve the problem related security vulnerabilities of cloud computing. Therefore, in order to build a cloud-based secure command control system, it is necessary to derive

※ 이 연구는 국방과학연구소의 국방 지휘통제 통합·연동 기반기술 특화연구실 과제의 지원을 받았습니다(UD180012ED).
◆ First Author : Security Engineering Lab, Dept. of Computer and Information Security, Sejong Univ., sigmao@naver.com, 학생회원
° Corresponding Author : Security Engineering Lab., Dept. of Computer and Information Security, Sejong Univ., alwaysgabi@sejong.ac.kr, 정회원
* Agency for Defense Development, shlee@add.re.kr
논문번호 : 201911-291-0-SE, Received October 25, 2019; Revised December 24, 2019; Accepted January 3, 2020

additional cloud computing-related security requirements that are lacking in the existing security requirements and to build the secure national defense command and control system architecture based on it. In this paper, we derive security requirements for cloud-based command control system and propose a security architecture designed based on it.

Ⅰ. 서 론

최근 사물인터넷(IoT), 빅데이터, 클라우드 기술로 인한 모든 사물이 인터넷으로 연결되는 초연결사회(Hyper-connected Society)로의 진입이 급속하게 진행되고 있다. 이에 따라 2010년부터 미국 등 주요국은 클라우드 우선 적용(Cloud First) 정책을 기반으로 정부·기업에서의 클라우드 이용이 급속 확산중이며 국방 및 공공부문 효율화, 국가혁신 추진, 클라우드 컴퓨팅 이용 환경 개선을 위한 인프라 구축 등을 추진중이다. 미 국방부는 여러 지역의 데이터센터들을 논리적으로 통합할 수 있는 클라우드 컴퓨팅으로 전환중이며, 합동정보환경(JIE; Joint Information Environment)의 목표 달성을 위하여 클라우드 컴퓨팅 접목에 지속적인 노력을 기울이고 있다. 한국에서도 '클라우드 컴퓨팅 활성화 추진계획('09)', '클라우드 컴퓨팅 확산 및 경쟁력 강화전략('11)'과 정부 3.0 발전계획('14) 중 '클라우드 컴퓨팅기반의 지능정부구현' 과제에 따라 정부부처는 클라우드 컴퓨팅 환경으로의 전환을 추진 중이다. 한국군은 국방정보자원 운용의 효율화를 위해 클라우드 컴퓨팅 도입의 필요성을 인식하고 육·해·공군의 전산소를 통합한 국방통합데이터센터를 설립하였으며, 전군 공통의 일부 시스템을 대상으로 클라우드 컴퓨팅 서비스를 제공하고 있다.

그러나 한국 국방부의 정보화 정책은 클라우드 컴퓨팅을 지향하고 있으나 아직은 초기 단계이며 클라우드 이용방안 등에 관한 세부 정책 및 제도가 마련되지 않은 상황이다. 또한 한국군 내부의 각 군 체계마다 사용되는 보안플랫폼, 보안통신프로토콜, 보안솔루션 등이 서로 상이하기 때문에 지휘통제체계(C4I; Command, Control, Communication, Computers and Intelligence)의 종합적·전사적 관제 및 대응이 어렵다. 특히 체계별 상이한 IdAM(Identity and Access Management)을 운영하고 있어 제공하는 인증, 인가 및 접근통제 수단과 과정이 다르기 때문에 각 체계별 검증된 보안을 제공하는지 확인이 어렵다. 예를 들어, 체계별 IdAM이 동일한 인증 수단으로 암호모듈을 사용하여도 이를 인증하는 과정은 각 IdAM마다 다를 수 있으며 각각 별도의 유지보수가 필요하다. 또한 체계 간 연동 시 신원정보, 크리덴셜 및 속성 등 인증에 필요한 요소들의 사용에 대한 일치가 필요하다. 현재 클라우드 컴퓨팅 환경에서는 기존 컴퓨터 시스템 환경과 유사하지만 다른 새로운 보안 취약점들이 발생하고 있으며 기존의 보안 시스템으로는 적절한 대응이 어렵기 때문에 클라우드 컴퓨팅 기반의 안전한 국방 정보시스템을 위해서는 추가적인 보안 요구사항이 도출되어 적용되어야 한다[1,2].

따라서 미군이 클라우드 컴퓨팅 도입 시 적용한 보안 요구사항들과 기존의 한국군 정보시스템의 보안 요구사항과 클라우드 컴퓨팅 시스템의 보안 요구사항을 분석하여 한국군 클라우드 기반 정보시스템에 필요한 보안 요구사항 도출이 필요하다. 또한 도출된 보안 요구사항을 기반으로 클라우드 기반의 안전한 미래 한국군 C4I 체계 구축을 위한 보안 아키텍처 설계가 필요하다. 본 논문에서는 현 한국군의 정보시스템 보안 요구사항이 기술된 훈령을 분석하여 추가적인 보안 요구사항들을 도출하였으며, 이를 기반으로 클라우드 기반의 C4I 보안 아키텍처를 작성하고 인증 및 접근통제에 초점을 맞춘 C4I 운영적 관점(OV; Operational View)을 제안한다. 본 제안하는 보안 아키텍처는 클라우드 기반의 중앙집중형 IdAM을 가지며 인증, 인가 및 접근통제의 일관성을 제공하여 신원정보 및 크리덴셜 관리의 용이성과 체계 별 유지보수 비용 절감 등을 이룰 수 있다.

본 논문은 제2장에서 현 한국군과 미군의 국방 C4I 환경과 보안 요구사항을 분석하고 제3장에서 클라우드 기반 C4I 보안 요구사항을 도출하며 제4장에서 도출된 보안 요구사항을 기반으로 미래 한국군의 클라우드 기반 C4I 보안 아키텍처를 제안한다. 제5장에서는 기존의 C4I체계와 제안한 보안아키텍처를 비교 평가하며 제6장에서는 결론과 향후연구에 대하여 설명한다.

Ⅱ. 배 경

본 장에서는 현 한국군과 선진국의 국방 C4I 환경에 대하여 분석한다. 현 한국군 환경으로는 현재 적용

되어 사용되고 있는 한국군 정보시스템 보안 요구사항과 한국군의 C4I 간 연동을 분석하며 선진국 국방 환경으로는 현재 미 국방부가 사용하는 클라우드 인증제의 보안 요구사항을 분석한다.

2.1 현 한국군 국방 지휘통제체계 환경

본 절에서는 기존 한국군 정보시스템의 보안 요구사항이 명시된 '국방사이버안보훈령'과 현 한국군의 C4I 간 연동을 분석한다. 그러나 한국군 정보시스템의 보안 요구사항이 명시된 '국방사이버안보훈령'과 현 한국군의 C4I 간의 연동 절차는 기밀 사항으로서 공개되지 않으므로 분석 내용은 일부 필요 보안 조치 사항만 제한적으로 설명한다.

2.1.1 현 한국군 정보시스템 보안 요구사항

현재 한국군의 국방 보안 관련 훈령으로는 '국방사이버안보훈령', '국방보안업무훈령', '국방정보화업무훈령' 등이 있으며 각 훈령들은 연관되어 다른 법률 등에서 파생되고 참조된다. 이 중에서 한국군의 정보시스템을 위한 보안 요구사항은 '국방사이버안보훈령'에 별첨되어 있으며 5개의 정보보호분야와 237개의 상세 요구사항이 존재한다. '국방사이버안보훈령'은 정확하고 안전하며 효과적인 국방사이버공간을 창출·유지·보호하고, 적대세력에 비해 사이버공간의 우위를 확보하는 것을 목표로 하는 제반 업무에 대해 지침과 절차를 규정함을 목표로 한다. '국방사이버안보훈령'의 정보시스템 보안요구사항의 5가지 정보보호분야로는 네트워크 보호, 서버 보호, 단말기 보호, 응용체계 보호, 보호 관리가 포함된다. 국방정보시스템은 기밀성, 무결성, 가용성 측면에서 자산의 중요도와 위험을 판단하여 '가', '나', '다'급으로 분류되는데 각 분야별 상세 요구사항들은 국방정보시스템의 중요도에 따라 분류될 수 있으며 표 1과 같다.

표 1. 국방사이버안보훈령 보안요구사항 분야와 보안수준
Table 1. Security Requirements Field and Security Level of the Korea National Defense Information System

	Security Field	Security Level		
		A	B	C
Security Requirements	Network Security	-	-	-
	Server Security	-	-	-
	Personal Computer Security	-	-	-
	Application Security	-	-	-
	Security Management	-	-	-

현재 '국방사이버안보훈령'에 명시된 국방 정보시스템 보안 요구사항은 클라우드 접목 시 필요한 보안 요구사항이 결여되어 있으며 크게 가상화에 대한 요구사항과 클라우드 서비스 자산관리에 대한 보안 요구사항의 추가적 적용이 필요하다.

2.1.2 현 한국군 지휘통제체계 간 연동

현재 한국군의 C4I는 연합지휘통제체계(AKJCCS; Allied Korea Joint Command Control System), 합동지휘통제체계(KJCCS; Korean Joint Command and Control System), 지상전술지휘통제체계(ATCIS; Army Tactical Command Information System), 해군전술지휘통제체계(KNCCS; Korea Naval Command Control System), 공군전술지휘통제체계(AFCCS; Air Force Command and Control System), 대대급 이하 C4I 등으로 구성된다. 각 체계 간 운용하는 시스템이 다르며 육·해·공 체계는 상호 간의 연동이 제한적이고 KJCCS와의 연동을 거쳐 자료 공유를 가진다. 본 절에서는 KJCCS와 ATCIS와의 연동 시 필요한 보안 조치 사항에 대하여 분석한다.

현 한국군에서는 체계 사용자가 먼저 암호모듈을 발급받고 시스템에 등록 과정을 가져야한다. 또한 각 군 체계별 키 관리체계가 구축되어 있기 때문에 체계별 ID, 비밀번호와 암호모듈을 사용해야 하며 각 체계마다 연동라우터 및 연동서버를 별개로 가져야 한다. 따라서 ATCIS 사용자가 KJCCS에 접근하기 위해서는 ATCIS용 ID, 비밀번호와 암호모듈로 인증을 받고 추가로 KJCCS용 ID, 비밀번호로 인증해야 한다. 이러한 과정은 체계별 자료 교환 시 암호해제로 인한 보안성 저하 및 운용의 편의성 제한을 가지며 직접적인 체계 간의 상호운용성을 가지지 못한다.

2.2 선진국의 국방 클라우드 보안 요구사항

미 국방부는 최근까지 시스템마다 서로 다른 어플리케이션, 엔클레이브(Enclave), IdAM을 운영하였다[3]. 현 한국군의 암호모듈과 같이 공통 인증 수단인 CAC(Common Access Card)를 사용하였으나, 각 체계 별 인증, 인가 및 접근통제 과정이 달라 비일관성 문제가 발생하였다. 또한 이러한 체계별 다른 IdAM을 운영할 경우, 각 체계의 구성이 검증되었는지에 대한 확인이 필요하다. 그렇기에 현재 미군은 정보 교류와 데이터 접근의 보안을 강화하기 위해 JIE를 택하고 JRSS(Joint Regional Security Stacks)를 배치하는 클라우드 기반 국방 정보시스템을 구축 중에 있다. 또한 FedRAMP (Federal Risk and Authorization

표 2. FedRAMP 보안 요구사항
Table 2. FedRAMP Security Controls Baseline

Name	Requirements
FedRAMP Security Controls Baseline	Access Control
	Security Alert and Education
	Inspection and Responsibility
	Evaluation and Authorization
	Configuration
	Emergency Management
	Identification and Authentication
	Incident Response
	Maintenance Management
	Media Security
	Physical Environment Defense
	Plan
	Personnel Security
	Calculate Threat
	Add System & Service
	System & Communication Security
	System & Information Integration

Management Program)와 미 국방정보체계국(DISA; Defense Information System Agency)의 클라우드 컴퓨팅 보안 요구사항 가이드를 통해 클라우드 컴퓨팅의 보안 요구사항을 도출하고 지시하고 있다. 표 2는 FedRAMP의 보안 요구사항이며, 표 3은 DISA의 클라우드 컴퓨팅 보안 요구사항을 나타낸다[4, 5].

미 국방부는 FedRAMP를 통해 클라우드 제품 및 서비스의 보안 평가, 인증 및 지속적인 모니터링을 위한 표준 접근방식을 제공한다. 미국 정부에 제품 및 서비스를 제공하려는 클라우드 서비스 제공 업체는 FedRAMP 규정 준수를 인증해야하며, FedRAMP 요구사항은 NIST 800-53, '연방 정보 시스템 및 조직의 보안 및 개인 정보 보호'에 지정된 요구사항이다. 표 2는 이러한 17가지 보안 요구 사항을 나타낸다.

또한, 현재 2,000개가 넘는 미국 정부 기관에서 다양한 AWS(Amazon Web Service)를 사용하고 있으며 미 국방부는 데이터를 처리, 저장 및 전송하기 위해 AWS를 적용하고 있다. AWS는 미 국방부 아래 DISA의 인증을 통해 미 국방부의 보안 요구사항을 준수하고 있으며 DISA는 표 3과 같이 보안 요구사항 가이드를 정의하고 표준 평가 및 인증 프로세스를 제공한다.

표 3. DISA 클라우드 컴퓨팅 보안 요구사항 가이드
Table 3. DISA Cloud Computing Security Requirements Guide

Name	Requirements
DISA Cloud Computing Security Requirements Guide	Availability Assurance
	Usage of SSL/VPN
	Recovery(Duplexing, Backup)
	Security Team Composition
	Resilience, on-Demand Scalability
	Maintain Operational Transparency
	Personnel Security
	Logical Separation of Information Data
	Physical Separation of Information Data

2.3 선진국의 국방 클라우드 보안 요구사항

현재 한국 국방부에서는 클라우드 도입을 위해 각종 시범 사업 및 확산정책을 수립하여 추진하고 있다. '국방 클라우드 확산 정책연구'에서는 국내·외 클라우드 정책 및 추진실태를 분석하고 국방 클라우드 추진 전략을 제시한다. 추진전략으로는 국방 클라우드 적용 사례 분석, 국방 클라우드 적용 확산을 위한 법·제도·훈령 개선 소요 제시, 클라우드 유형별 적용 방안 제시 등이 포함되며 국방 4차 산업혁명과 클라우드 적용 방안에 대해 제시한다. 미 국방부에서도 합동 방어 인프라(JEDI; Joint Enterprise Defense Infrastructure) 프로젝트를 통해 미국 국방부 및 임무 파트너들에게 IaaS(Infrastructure as a Service) 및 PaaS(Platform as a Service)를 포괄하는 기업 수준의 상업적 클라우드 서비스 제공을 목표로 하고 있다. 또한, JEDI 클라우드 요구사항에 대하여 설명하며 국방 클라우드의 주요 목표를 달성하려고 한다. [6]의 저자는 한국형 전투 클라우드 구축의 필요성 및 방안에 대하여 설명한다. 전투 클라우드란 다중 전투공간에서 모든 전투원과 전투 플랫폼 및 노드가 투명하게 필수적 정보를 군사작전의 전 범위에 걸쳐 활용하는 데이터 분배 및 정보 공유 그물망을 의미한다. 저자는 전투 클라우드가 가져야하는 구조에 대한 분석과 앞으로의 구축 방향에 대하여 설명한다. [7]의 저자는 국방 분야의 클라우드 적용이 국방 업무 특성 및 각 군의 정보시스템 운용의 다양성 등의 많은 제한사항들로 인하여 현실적인 적용의 과정은 쉽지 않다고 말하며 국방 클라우드의 확산을 위한 정책 방향과 전략을 제시하고 있다.

Ⅲ. 클라우드 기반 국방 지휘통제체계 보안 요구사항 도출

본 장에서는 기존 한국군 정보시스템의 보안 요구사항과 미군의 국방 클라우드 보안 요구사항을 참조하여 클라우드 기반 미래 한국군 C4I 시스템이 추가적으로 갖추어야 할 보안 요구사항을 도출한다. 보안 요구사항 도출을 위하여 '클라우드 서비스 보안 인증제 안내서(한국인터넷진흥원)'[8], '서버 가상화 시스템 보안 요구사항(한국정보통신기술협회)'[9], '국가·공공기관 클라우드 컴퓨팅 보안 가이드라인(국가정보원)'에서 식별한 클라우드 보안 요구사항을 참조한다. 도출된 보안 요구사항은 표 4와 같으며, 크게 가상화보안, 데이터보호, 네트워크보안, 접근통제, 위험 관리 분야로 나누어지고 총 28개의 항목을 가진다.

표 4. 클라우드 기반 국방 C4I 체계 보안 요구사항
Table 4. Security Requirements for Cloud-based National Defense C4I System

Division	Security Requirements
Virtualization Security	Establishment of management plan for creation, modification and recovery of virtual resources (virtual machines, virtual storage, virtual software, etc.).
	Monitoring of protection measures and changes (modifications, moves, deletions, and copies) of virtual resources to ensure the integrity of the virtual resources. Notify users and administrators when a virtual resource has been damaged.
	Provide access control measures for the hypervisor's functions and interfaces to manage virtual resources, and keep software updates and security patches up to date on the hypervisor.
	Supports security technologies such as malware detection and blocking to protect users' virtual environments (virtual PCs, virtual servers, virtual software, etc.) from malicious codes such as viruses, worms, and Trojan horses.
	Periodically analyze and protect security vulnerabilities on interfaces and APIs for accessing virtual environments (virtual PCs, virtual servers, virtual software, etc.).
	Monitor and manage the identification, tracking and survival cycles for virtual machine.
	Keep the initial component settings of the virtual machine unchanged.
	Monitors the traffic passing through the virtual machine by utilizing the virtual machine-specific mechanism built into the API.
	Maintain usage lists for virtual resources such as virtual machines, virtual storage, and virtual applications.
Data Security	Preventing information leakage of the guest operating system.
	Prepare technical measures such as encryption, management policy for information assets, and management of information asset list to safely transfer data when existing information system environment is changed to virtual environment of cloud computing service.
	Use different encryption keys in different environments such as cloud computing development, testing, and operations.
	Use military-certified encryption algorithms when encrypting data.
	The cloud computing system management organization should allow users to change keys at regular intervals.
	Take measures to ensure the confidentiality of data when moving data between cloud servers and storage or storage and storage.
	Implement mechanisms to validate input and delivery information in cloud computing systems.
	Duplexing critical equipment such as network switches and storage, and periodic backups by storing images and snapshots.
	Control and manage information flow within and outside the cloud system.
Network Security	Provides protection for distributed denial of service.
Access Control	Establishment of appropriate control policy and security technology considering the access situation from portable and mobile devices to cloud computing service.
	Identify users and administrators who have access to the cloud computing system and establish procedures for

	authorization and revocation of duties.
	Block unauthorized data transmission and reception between cloud access devices and cloud computing environments.
	User authentication, monitoring and integrated management of wireless access to cloud services are required.
Risk Management	Controlling users owning multiple sessions simultaneously in a cloud computing service environment.
	In cloud computing systems, monitoring targets and locations must be defined, software operation is regularly monitored to detect unintended changes in software, and reassessment activities are conducted through integrity checks.
	In the error event, identify the cause of the error quickly and ensure that critical information for the system is not disclosed in the error message.
	The cloud system manager should identify the cause of the security incident based on the collected monitoring data, and establish a plan to respond promptly to future security incidents.
	Each military information security system manager should establish and implement security measures against hacking of data and falsification when a virtual server is operated.

가상화 기술과 관련된 보안 요구사항으로는 가상머신, 가상스토리지, 가상서버, 가상소프트웨어 등과 같은 가상자원에 관련된 항목이 필요하다. 가상화 보안은 서버, PC(단말기), 응용프로그램에 각각 적용되며 서버 가상화 보안에는 하이퍼바이저 보안, 공개서버 보안이 포함되고 응용프로그램 보안으로는 가상소프트웨어 보안이 포함된다. 하이퍼바이저 보안은 가상자원을 관리하는 하이퍼바이저의 기능 및 인터페이스에 대한 접근 통제 방안에 관한 요구사항이며 공개서버 보안은 가상자원을 제공하기 위한 웹사이트와 가상소프트웨어(어플리케이션, 응용프로그램 등)를 배포하기 위한 공개서버에 대한 물리적, 기술적 보호대책에 관한 요구사항이다. 가상소프트웨어 보안은 클라우드 컴퓨팅 서비스 제공자가 출처, 유통경로 및 제작자가 명확한 소프트웨어로 구성된 가상환경을 제공해야 하는 요구사항이다. 또한 세 항목에 공통적으로 가상환경에서의 악성코드 통제와 인터페이스 및 API 보안이 포함된다. 클라우드 컴퓨팅 시스템 자원 관리를 위한 보안 요구사항에는 클라우드 컴퓨팅에 사용되는 정보시스템, 정보 보호시스템 등과 같은 정보자산 식별, 보안 등급에 의한 관리, 지속적인 모니터링 등이 포함된다. 또한 가상자원의 생성, 변경, 회수 등에 대한 관리와 가상자원에 대한 무결성을 보장하기 위한 보호조치 및 가상자원 변경에 대한 모니터링이 필요하다. 또한, 클라우드 컴퓨팅 서비스에 접근하는 사용자와 단말 등에 대한 분별된 권한 부여와 절차가 필요하며 알맞은 통제정책 및 보안기술 방안이 수립되어 클라우드 컴퓨팅에 대한 위험 관리가 필요하다.

Ⅳ. 클라우드 기반 지휘통제체계 보안 아키텍처

본 장에서는 앞서 분석하고 도출한 보안 요구사항을 기반으로 클라우드 기반 미래 한국군 C4I 보안 아키텍처를 설계하고, 동작 절차 등을 설명한다. 본 논문에서 제안하는 클라우드 기반 C4I 보안 아키텍처는 그림 1과 같이 3계층의 보안 아키텍처로 구성되며, 실제 클라우드 시스템이 도입되었을 때를 가정한다. 클라우드 기반 C4I 보안 아키텍처는 클라우드의 가상화 부분과 물리적 부분으로 구성되며, 전 계층을 운영하기 위한 운영계층으로 구성된다. 가상화 계층은 가상어플리케이션 계층과 가상인프라스트럭처 계층으로 나뉜다. 가상어플리케이션 계층은 기존의 클라우드 컴퓨팅 시스템의 SaaS(Software as a Service)와 같으며 가상인프라스트럭처 계층은 기존 클라우드 컴퓨팅 시스템의 IaaS와 같다. 그림 1의 좌측인 'Cloud based C4I system'은 클라우드 기반 미래 한국군 C4I체계를 나타내며 우측의 'C4I Security Architecture'는 C4I 체계 각 계층의 보안적 요소를 나타낸다. Virtual Application Layer에는 엔터프라이즈 서비스, 문서 공유, 프린터, 이메일, 웹 서버 등의 체계 이용자가 사용할 수 있는 서비스 요소가 해당되며, 해당 계층을 위한 보안 요소로는 웹 브라우저 보안 및 웹 인증이 포함된다. Virtual Infrastructure Layer에는 각 군에서 할당받을 수 있는 가상 환경 및 가상화 네트워크, 저장소, 서버 등이 포함되며 해당 계층을 위한 보안 요소로는 VM sprawl과 VM escape 공격과 같은 요소가 포함된다. Physical Layer는 실제 데이터 센터에 존재하는 물리적 장치들이 포함되며 저장 데이터의 안전성 및 네트워크와 서버 등의 물리적 보안 요소가 포함된다. 이러한 3계층을 통합적으로 관리하는 Operational Layer가 필요하며 보안 요소로는 정책 및

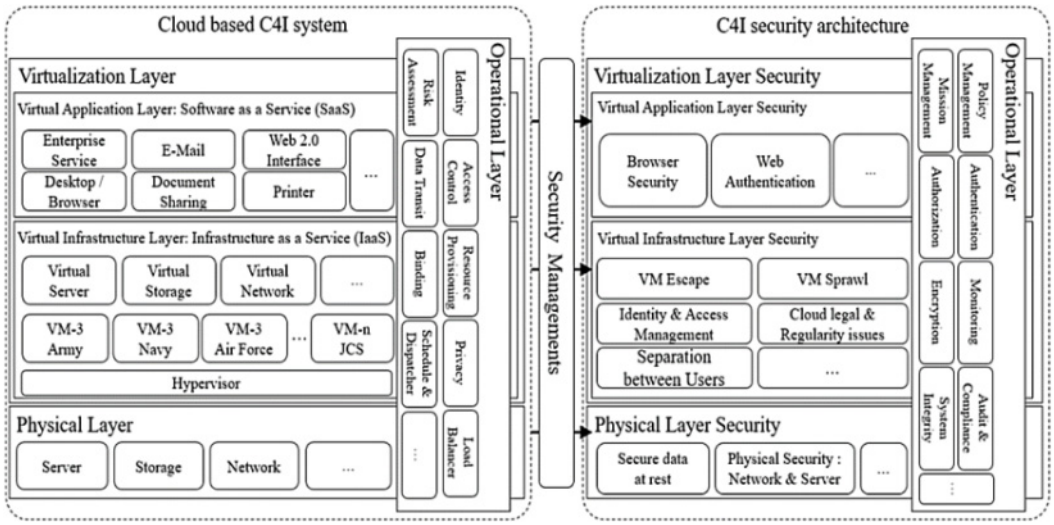

그림 1. 클라우드 기반 한국군 C4I 보안 구조(안)
Fig. 1. Cloud-based Korea Military C4I Security Architecture

임무 관리, 인증 및 권한부여와 같은 접근통제, 모니터링 및 심사, 통신 데이터 및 저장 데이터의 안전한 암호화가 필요하다.

도출된 보안요구사항과 아키텍처를 기반으로 미래 한국군의 클라우드 인증 및 접근통제 OV를 작성하였으며 그림 2와 같다. 그림 2의 요소로는 전군 사용자, 한국군 C4I 시스템, 인증 시스템, 인가 시스템, 신원정보서버, 정책서버, 키관리체계, 군 서비스가 존재한다. 한국군 C4I 시스템은 웹 브라우저와 같이 통합데이터 센터에 사용자의 접근을 가능하게 하는 역할을 한다. 또한, 그림 2의 1부터 9까지는 등록된 사용자의 인증 과정을 나타내며 10부터 17까지는 사용자의 군 서비스에 대한 요청과 권한 확인 과정을 나타낸다. 인증 시스템에는 사용자에 대한 ID, 비밀번호 등과 같은 기본 인증과 생체정보와 같은 다 요소 인증이 포함된다. 기본 인증과 다 요소 인증에는 신원정보서버와 키관리체계가 사용된다. 인가 시스템은 정책서버의 정보를 활용하여 사용자가 서비스를 요청했을 경우, 확인하여 서비스 사용을 허가한다. 또한, 서비스의 기밀 수준에 따라 다 요소 인증을 추가적으로 진행할 수 있으며, 이러한 경우에는 군 사용자의 미션 정보, 계급 등의 신원 정보를 참조할 수 있다.

V. 평 가

본 장에서는 기존의 C4I 체계 간 연동 과정과 새롭

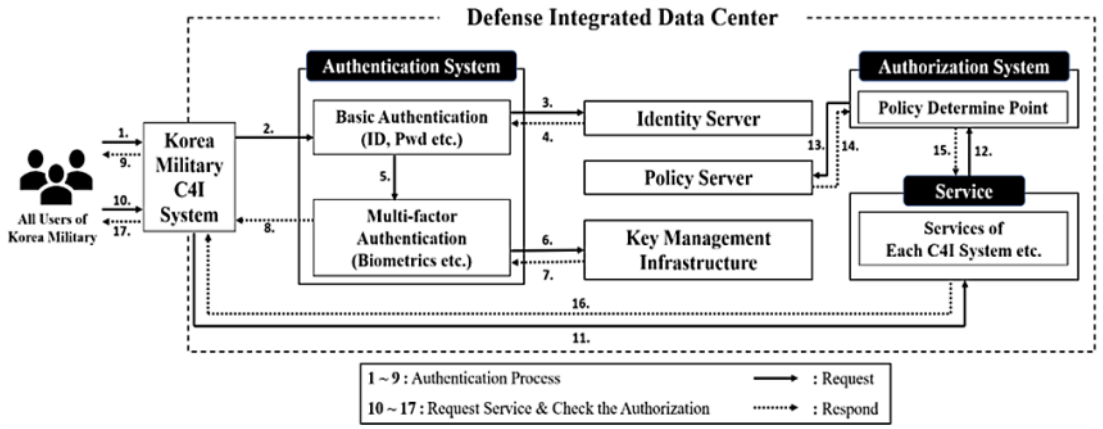

그림 2. 클라우드 기반 미래 한국군 C4I 인증 및 접근통제 운용적 관점
Fig. 2. Authentication and Access Control of Cloud-based Future Korea Military C4I

표 5. 기존 C4I 체계와 클라우드 기반 C4I 체계 비교표
Table 5. Comparison between Existing C4I system and Cloud-based C4I system

	Existing C4I System	Cloud-based C4I System
Interworking among Army/ Navy/ Air Force C4I Systems	Limited Interworking: Possible the interworking between KJCCS and other C4I systems,	Possible to access the any C4I service depending on the user's authority.
IdAM	Separated IdAM on each C4I system.	Centralized IdAM
Authenti-cation Factor	ID, Pwd for the user's C4I system, ID, Pwd for the KJCCS system and encryption module.	ID, Pwd and secondary authentication factor(biometric information, encryption module etc.)

게 제안하는 보안 아키텍처 OV 간의 비교 평가를 진행하며 표 5는 육·해·공 C4I 체계 간 연동, IdAM 형태, 인증 요소에 대한 차이점을 나타낸다. 또한, 클라우드 기반 C4I 체계와 기존의 일반적인 클라우드 환경과의 비교를 나타낸다.

기존 C4I 체계는 육·해·공 간의 연동이 제한되며 KJCCS와의 연동을 통하여 자료를 교환하며 각각의 C4I마다 IdAM이 존재하고 각 IdAM이 제공하는 인증, 인가 및 접근통제 수단과 과정이 다르다. 그러나 클라우드 기반의 C4I 체계에서는 각 체계 간의 데이터를 클라우드를 통하여 연동할 수 있으며 중앙 집중형의 IdAM을 가지기 때문에 인증, 인가 및 접근통제의 일관성을 제공할 수 있고 신원 정보 및 크리덴셜 값들을 관리하는데 용이하다. 또한 기존 C4I 체계에서는 사용자 인증을 위해 각 체계 사용자 ID, 비밀번호와 암호모듈 인증, KJCCS용 ID, 비밀번호가 필요하며 클라우드 기반 C4I 체계에서는 한국군 C4I용 ID, 비밀번호와 생체정보 또는 암호모듈과 같은 다 요소 인증요소가 필요하다.

클라우드 기반의 C4I 체계는 기존의 일반적인 클라우드 환경과 비교하여 구축 환경의 차이가 존재한다. 기존의 일반적인 클라우드 환경에서는 사용자의 구축 환경에 따라 퍼블릭 및 프라이빗 클라우드로 나뉜다. 그러나 클라우드 기반의 C4I 체계에서는 전시 상황에서의 사용을 가정하므로 프라이빗 클라우드 구축이 필요하다. 또한, 프라이빗 클라우드의 사용으로 기밀 서비스 사용에 대하여 네트워크 지연방지와 민감 데이터 관리에 대한 높은 성능 보장이 필요하다.

Ⅵ. 결 론

한국군은 클라우드 컴퓨팅 기술의 발전으로 국방 지휘통제 정보시스템에 클라우드 컴퓨팅 기술을 접목시키는 방향을 고려중이다. 그러나 기존 한국군 정보시스템의 보안 요구사항만으로는 클라우드 컴퓨팅 접목으로 인한 보안 취약점을 해결하는데 어려움이 있다. 그렇기에 미군의 사례를 참조하여 클라우드 보안 요구사항을 새롭게 추가 적용할 필요가 있다. 현재 국방 정보시스템 보안 요구사항은 클라우드 접목 시 필요한 보안 요구사항이 결여되어 있으며 크게 가상화에 대한 요구사항과 클라우드 서비스 자산관리에 대한 보안 요구사항이 추가적으로 적용되어야 한다. 또한 클라우드 환경에서의 데이터 보안, 네트워크 보안, 접근통제, 위험 관리 요구사항이 필요하며 도출된 보안 요구사항을 바탕으로 클라우드 기반 미래 한국군 보안 아키텍처를 설계하고, 인증 및 접근통제에 초점을 맞춘 OV를 제안하였다. 클라우드 기반 미래 한국군 보안 아키텍처는 가상화 계층, 물리적 계층, 운영적 계층으로 나뉘고 각 요소들에 대한 보안요소들로 구성된다. 인증 및 접근통제 OV에서는 기존의 C4I 체계와 다르게 중앙 집중식의 IdAM으로 사용자를 인증하고 서비스에 접근하는 시퀀스를 포함한다. 향후 연구로는 클라우드 플랫폼을 선택하여 군 예시 서비스에 대한 인증 및 접근통제 모듈을 개발하고 시험 평가하는 테스트베드를 구축 중에 있다.

References

[1] H. G. Kang, *The trend of U.S. cyber security market and Implication for advance of Korea corporations*(2016), Retrieved Oct. 18, 2019, from http://news.kotra.or.kr/user/reports/kotranews/20/usrReportsView.do?reportsIdx=6593

[2] G. D. Jung, *Operational Environment Construction of National Defense Cloud Computing*(2016), Retrieved Oct. 18, 2019 from http://www.prism.go.kr/homepage/theme/retrieveThemeDetail.do?leftMenuLevel=110&cond_brm_super_id=NB00012006120110005406O&research_id=1290000-201600115

[3] G. R. Lorenzo, *U.S. Army – Identity and*

Access Management (IdAM) Enterprise Reference Architecture (RA), Retrieved Oct. 21, 2019, from https:// ciog6.army.mil/Portals/1/Architecture/20140929-US_Army_Identity_and_Access_Management_Reference_Architecture_V4-0.pdf

[4] S. H. Gang, *Cloud Security Regulation of Major Countries*(2016), Retrieved Oct. 18, 2019, from https://spri.kr/posts/view/17533?code=information

[5] H. J. Lee and D. H. Won, "An analysis of cloud system security functional requirement," *J. Secur. Eng.*, vol. 9, no. 6, pp. 495-502, Dec. 2012.

[6] J. B. Kim and J. H. Park, "National defense cloud strategy and direction of development," *J. The Korea Soc. Inf. Technol. Policy & Management (ITPM)*, vol. 11, no. 2, pp. 1213-1220, Apr. 2019.

[7] C. I. Jeong, "Smart strategy for national defense in the fourth industrial revolution," *J. KICS*, vol. 36, no. 6, pp. 47-54, May 2019.

[8] KISA, *Cloud Service Security Certification Guide*(2017), Retrieved Oct. 21, 2019 from https://www.kisa.or.kr/public/laws/laws3_View.jsp?cPage=1&mode=view&p_No=259&b_No=259&d_No=91&ST=&SV=

[9] TTA, *Security requirements for server virtualization system*(2013), Retrieved Oct. 21, 2019 from http://www.tta.or.kr/data/ttas_view.jsp?rn= 1&pk_num=TTAK.KO-10.0708

구 자 훈 (Jahoon Koo)

2016년 2월 : 세종대학교 컴퓨터공학과 졸업
2017년 2월~현재 : 세종대학교 정보보호학과 석박통합과정
<관심분야> 사물인터넷 보안, 클라우드 컴퓨팅 보안

[ORCID:0000-0001-7481-9826]

김 영 갑 (Young-Gab Kim)

2001년 8월 : 고려대학교 컴퓨터학과부전공
2003년 8월 : 고려대학교 컴퓨터학과 석사
2006년 8월 : 고려대학교 컴퓨터학과 박사
2008년 3월 : 고려대학교 정보보호대학원 연구교수
2010년 1월 : 국가평생교육진흥원 선임전문원
2015년 2월 : 고려대학교 연구교수
2015년 2월 : 대구카톨릭대학교 IT공학부 조교수
2015년 3월~현재 : 세종대학교 정보보호학과 부교수
<관심분야> 전자공학, 통신공학, 광통신 공학
[ORCID:0000-0001-9585-8808]

이 상 훈 (Sang Hoon Lee)
1978년 2월 : 한양대학교 전자 공학과 졸업
1989년 2월 : 경북대학교 전자 공학과 석사
2002년 2월 : 충북대학교 정보통신공학과 박사
1978년 3월~현재 : 국방과학연구소
<관심분야> C4I 체계, 보안구조 연구
[ORCID:0000-0001-6857-2716]