논문 21-46-09-10 The Journal of Korean Institute of Communications and Information Sciences '21-09 Vol.46 No.09
https://doi.org/10.7840/kics.2021.46.9.1415

클라우드 기반 국방 정보시스템 구축에서의 정보보호 적용 방안 연구

진 정 하•, 김 병 준*, 한 근 희°

A Study on Applications of Information Security in Implementing Cloud-Based Defense Information Systems

Jungha Jin•, Byeongjun Kim*, Keunhee Han°

요 약

클라우드 기술의 발전으로 국방 분야에서도 정보시스템 구축시 활용방안에 대한 관심이 높아지고 있지만, 클라우드와 관련한 보안적인 이슈사항이 지속적으로 발생하고, 이를 보완하기 위해 다양한 연구가 진행중에 있다. 따라서, 정보시스템 도입과 관련한 국방 규정 및 훈령의 기준에 맞추어 국방 클라우드 정보시스템의 적용 방안을 도출하기 위하여 국내 및 국외의 클라우드 적용 방안에 대한 지침의 분석을 수행하고, 이를 기반으로 국방 클라우드 기반 정보시스템의 보안 개선 사항을 제시하고자 한다. 도출된 국방 정보시스템의 클라우드 도입시의 정보보호 개선사항 적용으로 선진국에 비해 다소 부족한 국방 분야에서의 클라우드 시스템 기술 도입시의 정보보호 이슈 사항에 대하여 개선방안을 제시하도, 향후에는 위험 관리 기반으로 클라우드 기반 정보시스템에서의 보안 통제 항목의 필수 적용 사항을 도출하는 연구를 제시하고자 한다.

키워드 : 클라우드, 사이버 보안, 국방 정보 시스템, 위험관리 프레임워크
Key Words : CLOUD, Cyber Security, Defense Information Systems, Information Security, Risk Manager Framework

ABSTRACT

With the development of cloud technology, interest in how to use it in the defense sector is also increasing. However, security issues related to the cloud continue to arise, and various studies are underway to compensate for them. Therefore, analysis such as guidelines for cloud applications both at home and abroad is carried out to derive a defense cloud-based information system application plan in line with the criteria of relevant defense regulations and instructions. Based on this, we will draw up information protection measures to introduce information protection measures for defense cloud-based information systems, present security improvements for defense information systems, and examine information protection considerations for cloud system technology. In the future, we would like to present a study that derives the essential application of security control items in defense cloud-based information systems based on risk management.

※ 본 연구는 2021년도 한화시스템(주)의 제원을 지원받아 수행된 연구임.
◆ First Author : KOREA University School of Cybersecurity Institute of Cyber Security & Privacy, nemoda75@korea.ac.kr, 종신회원
° Corresponding Author : KOREA University School of Cybersecurity Institute of Cyber Security & Privacy, khhan1@korea.ac.kr, 종신회원
* Air&Missile Defense System Team, Hanwha Systems Co. Ltd., byeongjun4037.kim@hanwha.com
논문번호 : 202107-165-B-RU, Received July 14, 2021; Revised July 27, 2021; Accepted July 28, 2021

Ⅰ. 서 론

클라우드 기반의 컴퓨팅 환경은 사용량 기반 지불 방식으로 인터넷을 통해 온디맨드 컴퓨팅 리소스를 전달하므로 컴퓨팅 역량을 전사적으로 확대하려는 조직에게 많은 보안상의 이점을 제공하고 있다. 대다수의 기업이 현재 약 20% 정도 클라우드 컴퓨팅 환경으로의 전환 작업을 진행하고 있으며, 이러한 기업들은 핵심 IT 인프라를 계속 현대화하고 미션 크리티컬 데이터와 앱을 클라우드로 이전하는 한편, 새로운 하이브리드 멀티클라우드 환경으로 인해 초래되는 고유한 사이버 보안 문제와 기회에 맞추어 클라우드 도입 및 운영 전략을 수정하여 조정해야 한다.

최근 가트너는 클라우드 보안에 대한 재평가를 통해 "고객의 실수로 인한 클라우드 보안장애가 99%에 달할 것이다." 라고 경고한 바 있으며, 이는 조금 과장되었기도 하지만, 클라우드가 미래 경제의 핵심이라는 부정할 수 없는 상황에서, 클라우드 보안은 진일보적인 기술로의 진화를 견고히 하기 위한 필수 요소임을 강조한 것이라고 볼 수 있다.[1] 데이터는 과거의 그 어느 때보다도 많이 축적되어 가고 있으며, 클라우드는 이러한 데이터의 무한한 증가를 부추기고 있고, 이러한 데이터의 증가로 인해 보안 이벤트 또한 기하급수적으로 증가하고, 이는 기존의 보안기술로 해결하기에는 역부족임에 따라서, 가트너는 이러한 현상을 "퍼블릭 클라우드 사용을 통제하지 못하는 조직 중 90%는 민감한 데이터를 부적절하게 다루고 있다"고 언급하고 있다.[1] 국제적으로도 데이터의 중요성과 개인정보 침해에 대한 이해도가 높아짐에 따라, 각 정부는 시민들의 권리를 보장하기 위한 법적인 규제를 더욱 강화하고 있어서, 데이터가 모여있는 클라우드 보안은 필연적인 과제이며, 향후에도 지속적으로 문제를 도출하고 해결방안에 대해 고민이 필요하다. 하지만, 퍼블릭 클라우드를 사용하는 조직의 49% 만이 중요 데이터를 암호화하여 사용하고 있는 현실이다.[2]

2019년부터 수집된 IBM Security 인시던트 대응 데이터에 따르면 클라우드 환경을 노리는 공격자의 가장 일반적인 동기는 금전적 이득이 대다수를 차지하고 있어서, 사이버 범죄자들은 일단 클라우드 환경에 침투하면 개인 식별 정보(Personally Identifiable Information, PII) 도용과 같은 데이터 절도 행위를 주로 하고 있다. 클라우드 애플리케이션에 대한 무차별 대입 및 익스플로잇 공격이 이 보고서에서 살펴본 사례의 45%를 차지하여 가장 일반적으로 사용되는 두 가지 감염 경로이며, 잘못 구성된 클라우드 서버를 활용함에 따라 2019년에 10억 개가 넘는 레코드 유출이 되는 사례도 존재한다. 2019년과 2020년 사이에 분석된 X-Force IRIS 인시던트 대응 사례에서 랜섬웨어는 클라우드에서 배포되는 가장 일반적인 유형의 멀웨어로, 2위와 3위를 차지한 크립토마이닝(암호 화폐 채굴) 및 봇넷 멀웨어보다 발생 건수가 3배나 더 많이 발생하였다.[3]

클라우드 서비스 플랫폼을 악의적 용도의 인프라로 활용하는 것은 노련한 공격자들이 즐겨 시도하는 방법으로서, 클라우드 고객 기업에 비용을 발생시킴으로써 공격자 자신의 비용을 최소화할 수 있으며 적법한 소스에서 비롯된 것처럼 보인다는 장점을 갖게 된다. 네트워크로 연결된 기존의 엔드포인트에 대한 랜섬웨어 공격과 달리 클라우드에서의 랜섬웨어는 더욱 파괴적인 영향을 끼치고 더 큰 데이터 손실을 초래하게 되는데, 그 이유는 클라우드 환경이 지원하는 운영의 범위가 훨씬 더 넓고, 중요한 애플리케이션에 잠재적으로 영향을 미치는 데다, 날마다 클라우드를 통해 이동하는 데이터의 양이 엄청나게 많기 때문이다. 공격자가 한 클라우드 환경을 감염시킨 뒤 신뢰할 수 있는 연결을 사용하여 다른 클라우드로 측면 이동한 후 추가로 환경을 감염시키는 방법으로 클라우드 환경을 침해하는 경우도 존재한다. 클라우드 환경, 특히 대규모 퍼블릭 클라우드는 많은 양의 통신이 이루어지므로 이러한 유형의 감염을 탐지하기가 훨씬 어려울 수 있기 때문에 클라우드 간 침해는 특히 은밀하게 진행될 수 있는 문제점을 갖고 있다. 이러한 유형의 공격을 통해 공격자는 여러 탐지 메커니즘을 피하고 자신의 활동을 일반적인 운영 활동인 것처럼 숨기면서 대규모 데이터 저장소 사이를 재빠르게 이동하여 대상 기업 전반에 해를 끼칠 수 있다.

이러한 클라우드 환경에서의 보안에 대한 문제가 존재함에 따라 국방분야에서의 클라우드 환경의 도입을 위해서는 정보보호 방안 도입이 필수적이며, 타 분야의 산업에 비하여 더 면밀하게 살펴보아야 한다.

본 논문에서는 국방 클라우드 기반 정보시스템의 안전성과 신뢰성 확보를 위한 정보보호 아키텍처를 구축할 수 있도록 하고, 현장에서 필수적으로 요구되는 보안 대책을 살펴보기 위하여 1장의 서론에 이어서, 2장에서는 클라우드의 개념을 기반으로 국방 분야에서의 클라우드 기술의 도입과 관련한 연구에 대하여 설명하고, 3장의 국방 클라우드 기반 정보시스템에서의 정보보호 적용 방안을 제시하고, 4장의 결론에서 향후 연구 진행방안을 설명하고 있다.

Ⅱ. 클라우드 기술 관련 연구

본 장에서는 국내외 클라우드 현황에 대해서 조사하여 분석함으로써, 현재 국방 분야에서 클라우드 기술이 적용시의 특징을 살펴보고자 한다. 클라우드 기반 국방 정보시스템은 시스템의 생존성을 우선적으로 고려해야 함에 따라서 주 사이트와 부 사이트의 이중화 구조에서 Active/Active 형태로 동작을 하며, 주 사이트의 장애 발생시 부 사이트에서 주 사이트의 작업 기기들을 이관 받아 운용하게 되는 구조로 동작하여야 한다. 이러한 클라우드 기반 국방 정보시스템의 도입을 위해 선진국의 클라우드 관련 문서들을 중점적으로 살펴본다.

2.1 FedRAMP (Federal Risk and Assessment Management Program)

미국에서는 공공분야의 클라우드 도입에 따라 보안에 대한 불신을 일소하기 위해 평가·인증 프로그램인 FedRAMP 도입하여 운영중에 있다. FedRAMP는 클라우드 컴퓨팅 서비스를 FISMA (Federal Information Security Management Act)에 적용하는 방식을 표준화하는 미국 정부 프로그램으로서, 2010년 12월 미국의 OMB (the Office of Management and Budget)는 “the 25 Points Implementation Plan To Reform Federal Information Technology Management” 에 기반하여 Cloud-First 정책을 수립하였다.[4-6]

Cloud-First 정책에서 다루고 있는 내용은 클라우드 컴퓨팅을 성공적으로 수행하기 위하여 클라우드 컴퓨팅 특성에 따른 정보보호 사안들을 다룰 수 있고 정부의 정보보호 수준에 맞는 프로그램이 필요하여 범 정부적 프로그램으로 클라우드 기반 서비스에 대한 보안평가, 인증, 지속적 모니터링을 제공하는 표준화된 프로그램임. FedRAMP는 FISMA 준수 비용을 줄이고 정부 기관이 정부 데이터를 보호하고 전례 없는 속도로 사이버 보안 취약점을 탐지 할 수 있다. 이를 위하여 FedRAMP에서는 연방 정보 클라우드 서비스 보호를 위한 연방 정부 정책을 수립과 FedRAMP의 개발, 구현, 운영 및 유지 관리에 대한 행정부 및 기관의 책임 정의 및 클라우드 서비스 취득 시 FedRAMP를 사용하는 집행부 및 대행사에 대한 요구사항을 정의하는 책임을 갖는 Office of Management and Budget (OMB)를 통해 정부 정책 및 우선 순위를 정부차원에서 이행하고 집행하는 거버넌스를 구현하여 정의하고 있다.

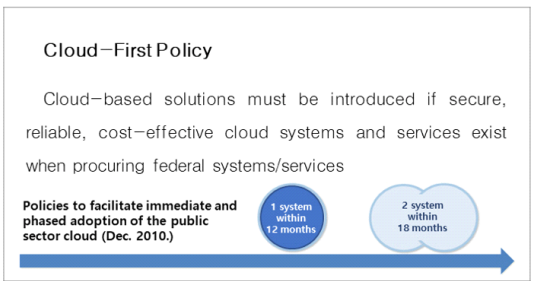

그림 1. FedRAMP Cloud-First 정책 개요
Fig. 1. Overview of FedRAMP Cloud-First Policy

이러한 FedRAMP 목적은 클라우드 기반 서비스에 대한 정보보호 적절성을 인증하고, 중복 투자 제거 및 위험관리 비용을 감소시키며, 신속하고 비용 효과적 연방정부 정보 시스템 및 서비스 조달체계를 구축하는데 있다. FedRAMP에서 다루고 있는 클라우드의 보안성 확보 방안은 보안평가 프레임워크인 SAF(security assessment framework)를 통해 이루어지고 있으며, FedRAMP SAF는 FISMA를 준수하며 NIST Special Publication 800-37 Rev.2를 기반으로 하고 있다.[7] FedRAMP는 클라우드 컴퓨팅의 고유 한 보안 요구 사항과 관련된 일련의 통제 기능 향상으로 개정된 NIST SP 800-53 Rev.5를 기반으로 하급 및 중급 보안 영향 시스템에 대한 통제 항목을 정의하고 있다.[8] FedRAMP의 보안통제항목은 NIST SP 800-53 rev.5에 규정되어 있는 통제 중 영향도가‘낮음’이나‘중간’수준의 시스템에 해당하는 보안통제를 기본으로 보완·수정하거나 클라우드 시스템 및 서비스 특수성에 의해 필요한 통제를 추가하여 사용한다.

2.2 NIST 클라우드 관련 문서

2.2.1 NISTIR 8320A

최근 클라우드 데이터 센터와 엣지 컴퓨팅에서, 공격 표면이 크게 증가하고, 해킹이 첨단화되며 대부분 보안통제 구현이 일관성을 가지지 않거나 지속적이지 않다. 데이터 센터나 엣지 컴퓨팅 보안 전략의 기반은 데이터와 작업이 접근되고 실행되는 플랫폼을 안전화해야 한다. 물리적 플랫폼은 계층화된 보안 접근법에서 첫 번째 계층이고, 상위-계층 보안통제가 신뢰될 수 있도록 초기 보호를 제공한다.[9]

해당 문서에서는 다중-임차 클라우드 환경에서 컨테이너 배치를 보호하기 위한 하드웨어-이용 보안 기술을 기반한 접근법을 설명한다. 또한 일반 보안 커뮤니티의 템플릿이 되는 접근법의 PoC(Proof-of-Concept) 구현

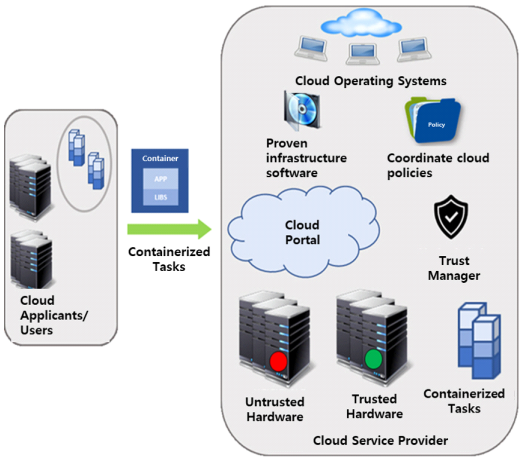

그림 2. 신뢰된 컴퓨팅 풀 개념도
Fig. 2. Trusted Compute Pool Conceptual Diagram

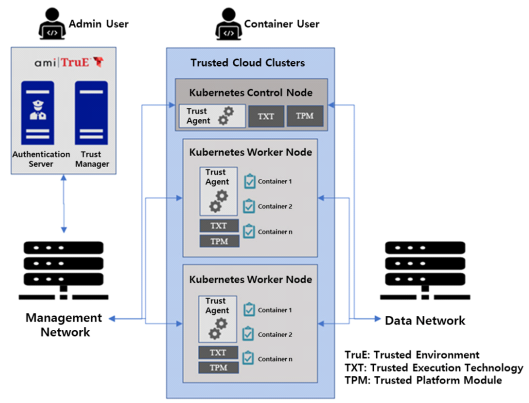

그림 3. AMI TruE 프로토타입 구현 개념도
Fig. 3. AMI TruE Prototype Implementation Conceptual Diagram

을 설명하고 있다.

2.2.2 NISTIR 8221

하드웨어/서버 가상화는 공유 시스템 자원을 접근하는 전사적 컴퓨팅과 클라우드 컴퓨팅 서비스를 사용하는 데이터 센터의 주요 기능이다. 서버 가상화는 일반적으로 하이퍼바이저에 의해 수행된다. 이 소프트웨어 계층은 물리적 하드웨어(하이퍼바이저 호스트)와 가상머신(VM, Virtual Machine)이나 GM(Guest Machine))에 실행되는 다중 애플리케이션 작업 사이에 위치한다. 하이퍼바이저는 가상 하드웨어 플랫폼에 운영체제를 제공하고 실행을 관리하는 VM을 지원한다. 그러나 하이퍼바이저는 수많은 코딩 라인과 취약성을 가진 대규모 소프트웨어임에 따라서, 클라우드 환경에서는 지속적으로 최신의 취약성을 기반으로 공격을 탐지/재구성/방지하기 위한 포렌식 분석 수행 역량이 아주 중요함에 따라서, 이 문서에서는 상기와 같은 클라우드 환경에서의 포렌식 분석을 수행하는 방법론의 개발을 목적으로 하고 있다.[10]

2.2.3 NISTIR 8006

클라우드 컴퓨팅 기술이 빠르게 적용되는 상황에서, 이 도메인에 디지털 포렌식 애플리케이션의 필요성이 부각되고 있다. 포렌식의 정당성과 신뢰성은 신규 환경에서 필수적이고, 빠른 공급, 글로벌 수요탄력성 및 광범위한 네트워크 접근성을 제공하는 다중-임차 클라우드 환경에서 증거를 식별/수집/보존/분석하기 위한 새로운 방법론이 필요하다. 보안사고 대응 및 내부 기업 운영 역량을 제공할 뿐만 아니라 형사/민사 소송 시스템을 지원하기 위해 필수적이다.[11]

NCC FSWG(NIST Cloud Computing Forensic Science Working Group)이 클라우드 환경에서 포렌식 문제를 연구하고 현재의 기술이나 개발된 방법론으로 해결될 수 없는 문제를 완화하기 위한 표준 기술 연구를 개발하기 위해 설립되었다. NCC FSWG는 클라우드 컴퓨팅 포렌식과 관련된 문제와 기존 문헌을 조사하여 관련된 문헌과 문제를 제시하고 있다.[12]

2.2.4 NISTIR 7966

사용자 및 호스트는 종종 아주 높은 권한으로 상호적이나 자동화된 방식으로 다른 호스트를 접근할 수 있어야 한다. 파일 전송, 재해 복구, 특권 접근 관리, 소프트웨어/패치 관리 및 동적 클라우드 제공을 포함하여 다양한 이유로 다른 호스트 접근은 종종 SSH(Secure Shell)을 사용하게 된다. SSH 프로토콜은 상호적이나 자동화된 인증을 위한 여러 가지 메커니즘을 지원한다. 이런 접근 관리는 정당한 제공, 폐기 및 모니터링 프로세스가 요구된다. 그러나 SSH 키-기반 접근 보안은 현재 상당히 간과되고 있다. 이 문서는 SSH 사용자 키에 초점을 두면서, 기업에서 SSH 상호적/자동화 접근 관리의 기본을 이해하는데 도움을 주고 있다.[13]

2.2.5 NISTIR 7956

클라우드의 다양한 서비스와 상호연계되어 동작하고 이런 서비스들이 생성하고 처리하는 데이터를 저장하기 위해, 다양한 보안 역량이 필요하다. 3 가지 공통 클라우드 서비스(IaaS/PaaS/SaaS)의 핵심 기능 세트를 기반으로, 이런 기능과 수반된 암호 작업을 실행하는데 필요한 보안 역량 세트를 식별한다. 이런 보안

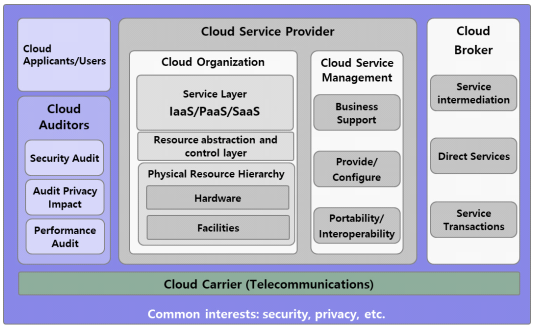

그림 4. 클라우드 컴퓨팅 보안 참조 아키텍처 접근법
Fig. 4. Cloud Computing Security Reference Architecture Approach

역량을 제공하는 암호 작업의 공통 사례 상태 분석에 의하면, 암호 키 관리가 소유권 차이(클라우드 소비자와 클라우드 공급자 간)나 KMS(Key Management System)와 보호된 자원이 위치한 인프라 통제와 같은 이유로 전사적 IT 환경과 비교하여 클라우드 환경에서 추가적인 복잡성을 유발한다고 확인되어진다. 이 문서에서는 이런 암호 작업을 수행하기 위해 일반적으로 적용되는 아키텍처 솔루션 환경에서 암호 키 관리 문제를 식별하고 있다.[14]

2.2.6 NISTIR 7904

이 문서는 IaaS 클라우드 컴퓨팅 기술과 지리적 위치를 포함하여 선택된 보안 문제를 설명하고 있다. 이런 문제를 처리하도록 지정된 PoC(Proof of Concept) 구현을 충분하고 자세하게 설명하고, 조직이 원한다면 재생성할 수 있도록 지원하고 있다. 서술된 PoC 구현을 검증하고 구축하기 위해 일반 보안 조직에서 사용 가능한 템플릿이나 청사진을 제시하고 있다.[15]

2.3 KISA 클라우드 서비스 보안인증제도

클라우드 서비스 보안인증제도는 클라우드 서비스 제공자가 제공하는 서비스에 대하여 정보보호 기준의 준수여부 확인을 인증기관이 평가하여 인증함으로서 이용자들이 안심하고 클라우드 서비스를 이용할 수 있게 지원하는 제도이다. 국방 클라우드에서는 객관적이고 공정한 클라우드 서비스의 보안의 적용을 위해서는 국내의 클라우드 보안인증제의 기준을 충족할 필요가 있으며, 이를 통해 사용자 신뢰도 향상 및 국방 클라우드 서비스에서의 정보 보호 수준을 향상시킬 수 있다. 인증 받은 클라우드 서비스를 이용함으로써, 국방 클라우드 도입에서 보안우려를 해소하고, 안전한 서비스 구축 및 이용의 활성화가 가능하다.[16]

클라우드 보안인증제도에서는 SaaS 시장이 영세한 중소사업자가 다수 차지하고 있으며 단일 IaaS서비스 위에 다수의 SaaS 서비스(3rd Party 등)가 동작하는 현실을 감안할 때 안전한 클라우드 서비스 이용을 위해서는 보안성이 확보된 SaaS 육성이 시급하여 공공기관에서 안심하고 사용할 수 있는 SaaS서비스 제공을 위하여 클라우드 보안 인증범위를 기존 IaaS에서 SaaS까지 확대하여 공공기관의 클라우드 이용 확산 및 클라우드 산업 활성화를 추진하고 있다.[17]

2017년 6월 기존의 IaaS 인증기준 대비 32% 감소(기존 117개 -> 78개)됨에 따라 IaaS 인증보다 신속하게 진행 가능(IaaS 4개월, SaaS 3개월), IaaS에 의존적인 물리적 보호조치 전체, 관리적 보호조치 일부 항목 삭제, 다자간 계약관계나 이용자 데이터 흐름 및 SW 개발 보안 등 강화, IaaS 평가방법 기반 SaaS 사업자 및 환경을 고려한 평가방법 마련 등을 반영하여 SaaS에 적합한 클라우드 보안인증기준 및 평가방법론을 마련하였다.

Ⅲ. 클라우드 기반 국방 정보시스템의 정보보호 적용 방안

클라우드를 활용한 기술 구현은 국방 산업에 있어 서비스 질, 운영 효율성 향상, 타 군과 정보 공유, 관리비용 절감 등 다양한 측면들의 개선을 불러일으킬 수 있다. 또 데이터 저장과 데이터 손실 예방, 군사 정보 기록 유지, 정보 공유 승인 등 다양한 방식으로 적용할 수 있다.

3.1 클라우드 환경의 국방 정보시스템 적용 필요성

클라우드 환경의 가장 큰 장점은 HW를 구매하지 않고 원하는 만큼 사용할 수 있다는 점에 있다. 이는 초기에 사용량에 대한 산정을 정확하게 하지 않아서 추가적인 재 구매로 인한 비용을 절감할 수 있다. 또한 국방은 다양한 환경의 시스템을 구축하고 변경해야 하는 상황에서 클라우드 시스템은 개발서버, 운영서버 등을 간단하게 설치 및 추가/제거를 진행 할 수 있다.[18]

클라우드, 빅데이터 등이 국방 사업에 도입되면 서비스 수준을 향상시킬 수 있다. 클라우드가 도입되면 국방 정보를 실시간으로 불러오고 활용할 수 있어서 정보시스템이 개선될 수 있고, 축적된 데이터들을 분석해 새로운 국방정보를 예측하고 확보할 수 있다.[19]

국방 사업에서 비용 절감과 서비스 품질 향상을 위해 그리고 수익을 더 높일 방안으로는 클라우드 환경이 가장 적합하다.

3.2 클라우드 기반 국방 정보시스템 특징

클라우드 기반 국방 정보시스템은 다중화 구조를 갖음으로서 생존성을 증대시켜야 한다. 극한 상황에서도 임무가 가능하도록 유지하는 생존성은 국방에서의 핵심 요소임에 따라서, 장애조치(Failover), 예비 사이트 전환(Site Takeover) 등을 통한 다중화 구조는 생존성을 증대시켜 국방 클라우드 정보시스템에서는 필수적인 요소로서 작용하게 된다.[19]

클라우드 기반의 국방 정보시스템은 클라우드 기반에서 구축되기 때문에 클라우드 환경의 특성을 그대로 유지하고 있다. 클라우드 기술은 공유, 단일화, 에뮬레이션, 절연의 기술을 기반으로 구현되고 있으며, 이러한 기술들을 통하여 물리적인 HW에 시스템을 구현하는 것이 아니고 가상환경에 시스템을 구축하고 운영할 수 있다.

가상화 환경에 국방 정보시스템을 구축하기 때문에 고가용성 및 리소스에 대한 효율적인 활용이 가능하며, 서비스 변화에 대하여 유연하게 대응할 수 있다. 공유기능을 통하여 물리적으로 분산된 자원을 나누어 사용할 수 있으며, 단일화를 통하여 물리적으로 나눠진 자산을 논리적으로 통합해서 사용할 수 있다. 에뮬레이션을 통하여 다양한 환경에서 개발되었더라도 동일하게 서비스를 구현할 수 있으며, 절연을 통하여 물리적으로 같은 서버에 구현되어 있다하더라도 정보의 유출을 예방할 수 있다. 클라우드 기반의 국방 정보시스템에서 사용하는 컨테이너 기술은 멀티테넌시 기술을 말하는 것이며, 멀티테넌시는 가상화와는 기술적으로 다른 특성을 가지고 있다.[20]

가상화는 서버 환경의 여러 가상 카피가 하나의 물리 서버에 의해 제공될 수 있으며, 각 카피는 다른 사용자에게 제공될 수 있고, 독립적으로 설정될 수 있으며 각 운영체제와 애플리케이션을 포함하고 있다. 멀티테넌시는 애플리케이션을 제공하는 물리 또는 가상 서버가 여러 다른 사용자가 사용할 수 있도록 설계되

표 1. 가상화 기술
Table 1. Virtualization Technology

	Sharing	Aggregation	Emulation	Insulation
Distinction	Make physically located resources available to users	Consolidate distributed resources to logically simplify, increasing resource utilization and facilitating management	Logical objects due to virtualization can perform the same functions as physical objects	Keeping services stable in the event of physical resource replacement or alteration
Related Tech.	- Partitioning - VLAN	- Clustering	- VTL - Emulator	- RAID - HA - L4 Switch

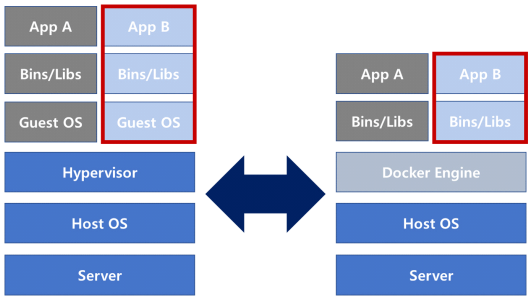

그림 5. 멀티테넌시와 가상화 기술
Fig. 5. Multi-Tenancy and Virtualization Technologies

며, 각 사용자는 애플리케이션을 배타적으로 사용한다고 느끼는 형태이다.[21]

단일 운영체제를 사용하는 환경에서는 멀티테넌시가 매력적인 선택이지만, 여러 운영체제를 구동해야 할 필요가 있는 환경에서는 가상머신과 하이퍼바이저가 유용한 방안이라고 볼 수 있다.

3.2.1 다중화 체계

클라우드 환경에서 가장 큰 장점 중에 하나인 서버 가상화 기술을 활용하여 물리적인 서버와 가상 머신을 고가의 특정업체 장비대신 일반적인 PC 서버 등을 활용하여 무제한 복제하여 서버 다중화를 안전하고 저렴하게 구현이 가능하다. 클라우드 환경이 아닌 기존 체계에서 실제 물리적인 서버를 운영하였듯이, 클라우드 환경에서는 가상머신들을 생성하여 운영가능함에 따라 물리적인 서버를 최소화 시킬 수 있다.

국방 클라우드 정보시스템에서는 작전서버 가상 머신에 문제가 발생할 경우 1차적으로 사전에 예비된 가상 머신으로 자동 장애조치(Failover)되고, 해당 물리적인 서버의 가상 머신에 모두 문제가 있다하더라도 물리적으로 이중화된 부 사이트의 Active 서버로 자동 장애조치(Failover)되는 구조로서 생존성을 극대화할 수 있다.[22]

3.2.2 다원화 체계

주 사이트 내의 모든 서버에서 문제가 발생하여 작전 업무가 불가능하게 될 경우에는 이원화된 체계인 부 사이트로 사이트 전환(Site Takeover)되도록 구현하여야 하며, 이를 위해서 가상화 기술과 네트워크 기술이 결합하여 데이터센터 간 가상 머신을 이동시키는 기술 구현이 가능해야 한다.

현재 국방 클라우드 정보시스템을 분권화시켜 주 사이트와 부 사이트 체계를 통해 작전 업무를 수행하고 있으나, 비상 상황을 대비하여 제3의 백업사이트

구축도 고려해야 한다.[23]

3.3 클라우드 환경의 국방 정보시스템에서의 정보보호 적용 방안

클라우드 환경에서는 다양한 보안사고가 발생하고 있으며, 이를 예방하기 위해서 클라우드 환경에 맞는 대응체계가 필요하다. 클라우드 환경은 동일 호스트상에 타인의 정보가 혼재되어 비인가자(내/외부)의 정보 접근 가능성이 더욱 증가한다.[24]

3.3.1 클라우드 기반 국방 정보시스템 보안 위협

사용자의 정보가 클라우드 서버 내 어디에 저장되고, 백업되고, 누가 접근하는지에 대하여 관리하는데 어려움이 존재한다. 더불어, 아마존 정전으로 11시간 장애 발생으로 190개 서비스 동시 마비 ('11) 사고와 아마존 AWS를 이용한 소니 플레이스테이션 네트워크 해킹 사고('11)를 보면 사고발생 시, 이용자 서비스 연쇄중단 및 대규모 피해가 발생하다.

특히, 클라우드 서버에 고객 정보 및 자원이 집적되어 해킹, DDoS 공격의 표적이 되거나 공격 경유지로 악용 되는 사례도 있다. 클라우드 환경의 보안위협은 기존의 보안 문제는 모두 발생할 수 있으며, 추가적으로 가상화로 인한 보안 위협과 중복된 신뢰경계로 인한 보안 위협이 추가 될 수 있음을 인지하여야 하다.

가상화로 발생할 수 있는 위협은 클라우드 서비스를 구동하기 위해 필수적인 가상화 시스템 내에 하이퍼바이저가 취약할 경우 이를 활용하는 여러 개의 가상머신이 동시에 피해를 입을 가능성이 있다. 사용자의 가상머신들이 상호 연결되어 내부의 가상머신에서 다른 가상머신으로 패킷을 스니핑 하거나 악성코드 전파 등의 공격 경로가 존재할 수 있다. 또한, 가상환경에서는 공격자가 누군지를 파악하기가 어려워 기존의 네트워크 보안기술로는 가상화 내부 영역에 대한 침입탐지 방안을 고려해야 한다.

신뢰경계의 중복을 살펴보게 되면, 기존에는 각 기업별로 안전하게 네트워크를 구성하여 사용 하였으나, 클라우드 환경은 다양한 사용자의 서비스를 물리적인 서버를 공유해서 사용하기 때문에, 물리적인 신뢰경계가 다양한 환경에서 중복이 발생할 수 있다.

이러한 환경에서 가상화로 인한 보안이슈가 발생하면 그 피해가 크게 발생할 수 있다.

결과적으로 클라우드 환경에서 효과적으로 보안을 하기 위해서는 기존의 보안체계 수준을 유지하고 추가적인 클라우드 환경에서 발생할 수 있는 보안 위협에 대한 대응방안을 마련해야 한다.

3.3.2 클라우드 기반 국방 정보시스템 보안 대응방안

클라우드 환경의 국방 정보시스템에 대한 사이버 보안을 위해서는 보안 위협을 식별하고 취약점을 제거하는 것과 동시에 다양한 위험 탐지 활동이 필요하다. 전통적인 구성에서 위험 탐지 활동을 위해서는 네트워크 레벨에서 보안장비를 구축하여 탐지 및 대응하였으며, 수직적 구조이기 때문에 상단 방화벽에서 악의적인 사용자를 차단하는 형태로 대응 하였다.

클라우드 환경은 수평적 구조로서 외부에서 유입되는 트래픽이 순차적으로 연결되지 않기 때문에, 기존과 같이 네트워크 경계에서 탐지 및 차단하는 것이 쉽지 않다. 기본적으로 물리적으로 보안을 구성하고 안전한 트래픽만 클라우드 내부로 유입되는 형태로 구성을 하고 있다. 클라우드 환경에서 기존과 동일하게 차단하기 위해서는 프록시를 구성하여 탐지 및 차단을 하거나 라우팅을 통하여 탐지 및 차단하는 방법이 필요하다.

클라우드 환경에서 서비스를 제공하면서 시스템에 패킷이 도달하기 전에 탐지 및 차단이 가능하다. 클라우드 서비스 제공자에 따라 방법은 조금식 다르지만 대부분의 클라우드 서비스는 서비스의 사용량에 따라 서버를 증가하고 감소시키는 기능을 제공하고 있다. 이러한 기능을 구현하기 위해서는 외부의 사용자는 VPN을 통해서 접근을 하게 되고 이러한 접근은 로드밸런서를 통하여 가상서버에 균등하게 배분한다. 결과적으로 외부에서 유입된 트래픽은 로드밸런서를 통하여 내부 시스템으로 유입 된다.

이와 같은 방식으로 기존의 전통적인 네트워크 경계에서의 보안통제와 동일한 수준의 보안통제를 클라우드 환경에서도 구현할 수 있다.

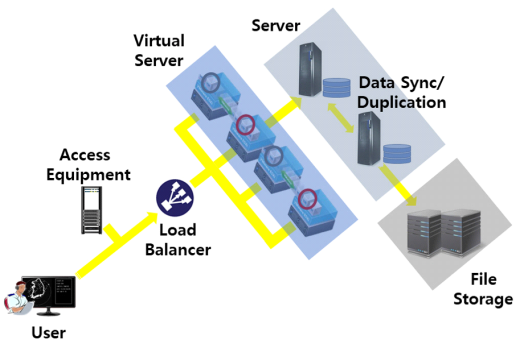

그림 6. 국방 프라이빗 클라우드 플랫폼 구성(예시)
Fig. 6. Configure Defense Private Cloud Platform (Example)

보안 솔루션을 이용한 클라우드 환경에서 보안통제는 기존의 전통적인 수준에서의 보안통제를 동일하게 구성하기 위한 방법이며, 클라우드 환경에서 추가적인 보안통제가 필요하다. 기본적으로 클라우드 환경에서 서비스를 구성하면 가상시스템이 수시로 생성/삭제가 발생되며 이를 실시간으로 통제가 가능해야 하다. 가장 큰 우려는 시스템에 설치된 보안 Agent가 가상 이미지를 통하여 가상시스템이 추가 되었을 경우 설치 및 설정을 자동으로 해야 하고 이후 management 시스템에 연동되고 관리 되어야 하다. Management 시스템은 서비스 시스템이 추가되고 삭제 되더라도 보안과 관련된 사항을 모니터링 하고 추적할 수 있어야 하다.

이러한 구성을 통하여 전통적인 방식의 보안통제를 클라우드 환경에서 동일한 수준으로 구현할 수 있으며, 추가적으로 클라우드 특성에 맞는 추가적인 보안통제를 구현할 수 있다.

3.3.3 클라우드 환경 국방 정보시스템 적용에 따른 정보보호 개선 방안

클라우드 환경의 국방 정보시스템 적용에 따른 정보보호 개선사항은 IaaS, PaaS, SaaS의 특성에 따른 보안통제 항목을 구성하여야 한다.

(1) IaaS 클라우드 환경의 국방 정보시스템 정보보호 개선 사항

아래의 표는 국방 IaaS와 관련된 보안통제항목들을 보여주고 있다. IaaS의 보호(Protect) 기능 통제항목들을 살펴보면 주로 네트워크, 스토리지, 시스템, 가상화(하이퍼바이저) 등과 관련된 범주의 통제항목들로 구성되어 있다.

보안통제항목별 내용은 통제목적, 적용내용, 국방 클라우드 정보보호 통제항목들로 구성되어 있으며, 국방 기능별 세부유형에 따라 적용내용을 보여준다.

표 2. 국방 IaaS 보안통제의 보안 등급 개요
Table 2. Overview of Security Ratings for Defense IaaS Security Control

Type	Essential	Recommendation	optional
Identify	2	4	0
Protect	11	5	6
Detect	1	3	2
Respond	0	3	2
Recover	0	2	1
sum	14	17	11

각 통제항목에 대하여 국내 관련법에서 요구하는 항목은 '필수(14)', 국내 관련법에서 요구하지 않는 항목 중에 클라우드 보안인증제에서 요구하는 항목은 '권고(17)' 그 외 항목에 대해서는 선택(11)으로 분류한다.

상기 표 2에서의 식별(Identity) 유형을 예로 들어 살펴보면 사업환경과 지침에 대하여 필수 항목으로 보안영역을 분류하고 있으며, 사업 환경에서는 아웃소싱 된 정보자산 및 시설에 대한 위험관리 프로그램 개발, 아웃소싱으로 개발된 소프트웨어 관리, 아웃소싱 된 정보자산 및 시설 인증 절차 마련, 사업연속성 관리체계에 정보보안 포함, 중요 서비스의 의존관계 및 주요 기능 파악, 주요 서비스의 복구 시 요구사항 정의, 타사 서비스 변경 관리가 적용내용에 포함되고, 지침에서는 조직의 정보보안 정책 수립, 정보보호 정책 문서 개발 및 검토, 정보보안 역할 및 책임 규정, 고용계약 상 정보보호 역할과 책임 명시, 적용되는 법규 확인, 정보보안 인식, 교육, 훈련 실시, 타사와의 계약에서 보안요구사항 명시, 내·외부 파트너와 사이버 보안 공동 대응 및 협력이 적용내용에 포함되고 있다.

아울러, 자산관리, 위험평가, 위험전략, 공급망 위험관리의 보안영역에 대하여 권고 사항으로 분류하고 있으며, 자산관리에서는 자산분류지침, 자산 및 자산 소유자 식별, 네트워크 구성도 보유를 통한 네트워크 분리 및 통제, 외부 정보시스템 목록 작성 및 관리/폐기 절차 마련, 직원의 역할과 책임 규정, 제3자 관련 위험 식별, 자산 목록화 작성 및 유지가, 위험평가에서는 자산 취약성 파악 및 문서화, 내·외부의 위협 식별 및 문서화, 사업적 영향 및 잠재적 기회 식별, 위험 식별, 우선 순위화, 문서화, 기술 준수 검사 및 기술적 취약성 통제, 아웃소싱으로 개발된 소프트웨어의 위험평가, 사업연속성 관리가, 위험전략에서는 위험관리프로그램 개발, 정보보안에 대한 독립적 검토, 사업연속성 관리, 위험의 수용가능범위 규정이, 공급망 위험관리에서는 사이버 공급망 위험평가 프로세스 수립, 정보시스템, 구성요소 및 서비스 공급업체, 제3자 파트너 식별 및 우선 순위화, 모든 관련 공급망에 대해 공급자와 소비자 간 보안수준계약(SLA)을 지속적으로 검토하기 위한 정책 및 절차 마련, SLA 체결 시 상호 합의된 서비스와 용량 기대 수준, IT 관리 방식, 서비스 관리 정책 및 절차 포함, 공급업체 및 제3자 파트너와의 계약서 상 사이버 공급망 위험관리 계획 포함, 사이버위험 대응 및 복구계획에 공급업체 및 제3자 파트너 포함의 적용내용이 포함되고 있다.

(2) PaaS 클라우드 환경의 국방 정보시스템 정보보호 개선 사항

아래의 표는 국방 PaaS와 관련된 보안통제항목들을 보여주고 있다. 국방 클라우드의 보호(Protect) 기능 통제항목들을 살펴보면 주로 운영체제(컨테이너), 미들웨어(개발환경), 런타임(로드밸런스) 등과 관련된 범주의 통제항목들로 구성되어 있다.

각 통제항목에 대하여 국내 관련법에서 요구하는 항목은 '필수(4)', 국내 관련법에서 요구하지 않는 항목 중에 클라우드 보안인증제에서 요구하는 항목은 '권고(15)' 그 외 항목에 대해서는 '선택(12)'으로 분류한다.

상기 표 3에서의 보호(Protect) 유형을 예로 들어 살펴보게 되면, 사용자 인증 및 권한 관리와 내부인력 보안에 대하여 필수 항목으로 보안영역을 분류하고 있으며, 사용자 인증 및 권한 관리에서는 사용자 등록 및 암호 관리, 비밀번호 사용, 외부에서 접속하는 사용자 인증, 네크워크 상 장비 식별, 보안 로그온 절차 수립, 사용자 식별 및 인증, 암호관리시스템 수립, 접근권한 부여·변경·철회, 네트워크 통제, 시스템 테스트 데이터 보호가 적용 내용에 포함되고, 내부인력 보안에서는 경영책임, 정보보안 인식 및 교육/훈련 실시, 정보보안 책임 및 절차 수립, 정보보안 책임 및 역할 이해가 적용 내용에 포함되고 있다.

아울러, 컨테이너 멀티테넌트 환경 보안, 안전한 개발환경 제공, 침해사고 대응 계획 수립을 보안영역 권고 사항으로 분류하고 있으며, 컨테이너 멀티테넌트 환경 보안에서는 컨테이너 이미지 취약점 및 악성코드와 평문 패스워드 사용점검, 컨테이너 이미지 환경설정 오류 점검, 허가되지 않은 네트워크 접근 및 컨테이너 탈출 등의 안전하지 않은 컨테이너 런타임 환경설정 점검이 적용 내용에 포함되고, 안전한 개발환경 제공에서는 개발 및 테스트 환경은 실제 서비스와 분리하여 제공, 개발환경에 사용된 취약점 제거, 개발환경 사용 종료 시 보안이 확보된 폐기절차 수립이 적용 내용에 포함된다. 또한, 침해사고 대응 계획 수립에서는 법적 수사를 준비하기 위해 법적 준수사항 모니터링, 침해사고 처리를 위한 정책과 절차를 확립하는 것이 적용 내용에 포함되고 있다.

(3) SaaS 클라우드 환경의 국방 정보시스템 정보보호 개선 사항

아래의 표는 국방 SaaS와 관련된 보안통제항목들을 정리하여 보여주고 있다.

SaaS의 보호(Protect) 기능 통제항목들을 살펴보면 주로 데이터, 어플리케이션(웹, 앱) 등과 관련된 범주의 통제항목들로 구성되어 있다. 보안통제항목별 내용은 통제목적, 적용내용, 국방 클라우드 정보보호 통제항목들로 구성되어 있다. 각 통제항목에 대하여 국내 관련법에서 요구하는 항목은 '필수(9)', 국내 관련법에서 요구하지 않는 항목 중에 클라우드 보안인증제에서 요구하는 항목은 '권고(15)' 그 외 항목에 대해서는 '선택(13)'으로 분류한다.

상기 표 4에서의 탐지(Detect) 유형을 예로 들어 살펴보게 되면, 탐지된 이벤트 분석, 추적 감사, 탐지절차의 지속적인 개선에 대하여 권고 항목으로 보안영역을 분류하고 있으며, 탐지된 이벤트 분석에서는 공격대상과 방법을 이해하기 위해 탐지된 이벤트 분석, 이벤트를 수집하고 연관분석 시행, 이벤트가 미치는 영향 파악의 내용이 적용 내용에 포함되고, 추적 감사에서는 데이터 복제와 액세스 및 데이터 경계 제한에 초점을 맞춘 감사 계획, 위반이 발생되는지 계획된 간격으로 수행, 비즈니스 요구에 따라 정기적으로 감사 계획을 업데이트를 수행하는 내용이 적용 내용에 포함된다. 마지막으로 탐지절차의 지속적인 개선에서는 탐지에 대한 책임과 역할 정의, 탐지 절차 테스트, 탐지 정보를 관계자와 의사소통, 탐지 절차의 지속적인 개선을 수행하는 것이 적용 내용에 포함되고 있다.

표 3. 국방 PaaS 보안통제의 보안 등급 개요
Table 3. Overview of Security Ratings for Defense PaaS Security Control

Type	Essential	Recommendation	optional
Identify	2	4	0
Protect	2	3	7
Detect	0	3	2
Respond	0	3	2
Recover	0	2	1
sum	4	15	12

표 4. 국방 SaaS 보안통제의 보안 등급 개요
Table 4. Overview of Security Ratings for Defense SaaS Security Control

Type	Essential	Recommendation	optional
Identify	2	4	0
Protect	2	3	7
Detect	0	3	2
Respond	0	3	2
Recover	0	2	1
sum	4	15	12

Ⅳ. 결 론

국방 환경에 글로벌 규모로 클라우드 컴퓨팅 및 데이터 저장소 같은 기반 기술을 제공하는 역량은 국가 안보와 전쟁 승리 준비에 필수적이다. 만일 국방이 한 단계 높은 차원으로 상대적인 우위성을 유지하고자 한다면, 인공지능 같은 기술을 활용할 필요도 있으며, 이를 위해서는 전사적 국방 클라우드 환경을 빠르게 구축할 필요가 있다.

이를 위하여 본 논문에서는 국방 클라우드와 관련하여 선진국의 클라우드 관련 기술과 국내의 클라우드 관련 내용을 기반으로 클라우드 환경에 대한 기본 개념을 살펴보고, 국방 클라우드를 이해하기 위해서 FedRAMP와 NISTIR 클라우드 관련 문건을 조사하였으며, 이를 기반으로 국내 클라우드 기반 정보시스템의 핵심기술인 가상화 기술과, 다중화 구조, 다원 체계에 대하여 간략하게 살펴서 현재 국방 현황에서 클라우드 기반의 정보시스템 도입에서의 보안 대응방안을 정리해 보았다.

국방 정보시스템의 클라우드 기술 적용시 보안 대응방안을 도출하기 위해 IaaS, SaaS, PaaS 에서의 정보보호 개선 사항을 도출하여 제시하고 있으며, 이를 기반으로 국내의 국방 클라우드 적용에 따른 정보보호 방안을 분석하고 개선 발전시킬 사항을 도출하여 정리하고 있다.

향후에는 미국방의 RMF와 국방 정보보호 지침 훈령의 매핑을 통해 실제 국방 클라우드 도입시 위협 분석 기반의 접근 방법 도입으로 시스템 구현시 보안의 안정성을 확보하는 방법에 관한 연구를 수행하고자 한다.

References

[1] K. Panetta, *Gartner offers recommendations for developing a cloud computing strategy and predictions for the future of cloud security*, https://www.gartner.com/smarterwithgartner/, Oct. 10, 2019.

[2] Ponemon Institute(2019), "*2019 Thales Global Cloud Security Study*," https://cpl.thalesgroup.com/, 2019.

[3] Cloud Threat Environment Report, *IBM Security X-Force IRIS*, 2020.

[4] *Security Assessment Framework*, https://www.fedramp.gov/documents-templates/, Nov. 15, 2017.

[5] *Federal Information Security Modernization Act of 2014*, PUBLIC LAW, pp. 113-283, Dec. 18, 2014.

[6] V. Kundra, *25 Points Implementation Plan To Reform Federal Information Technology Management*, U.S. Chief Information Officer, Dec. 9, 2010.

[7] SP 800-37 Rev. 2 : *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, NIST, Dec. 2018.

[8] SP 800-53 Rev. 5 : *Security and Privacy Controls for Information Systems and Organizations*, NIST, Dec. 10, 2020.

[9] NISTIR 8320A : *Hardware-Enabled Security: Container Platform Security Prototype*, NIST, Jun. 2021.

[10] NISTIR 8221 : *A Methodology for Enabling Forensic Analysis Using Hypervisor Vulnerabilities Data*, NIST, May 2019.

[11] NISTIR 8006 : *NIST Cloud Computing Forensic Science Challenges*, NIST, Aug. 2020.

[12] *NIST Cloud Computing Forensic Science*, https://www.nist.gov/programs-projects/nist-cloud-computing-forensic-science.

[13] NISTIR 7966 : *Security of Interactive and Automated Access Management Using Secure Shell* (SSH), NIST, Oct. 2015.

[14] NISTIR 7956 : *Cryptographic Key Management Issues & Challenges in Cloud Services*, NIST, Sep. 2013.

[15] NISTIR 7904 : *Trusted Geolocation in the Cloud: Proof of Concept Implementation*, NIST, Dec. 2015.

[16] *Cloud Security Assurance Program Gride*, KISA, Sep. 2020.

[17] *Cloud Security Assurance Program Evaluation Standard Explanation Guide*, KISA, Sep. 2020.

[18] C. Lim, et al., "A study on the technology and methodology of migrating from legacy command and control system to cloud computing environment," *J. KICS*, vol. 45, no. 2, pp. 428-436, Feb. 2020.

[19] D.-J. Kang, et al., “Cloud service broker technology and case study,” *KICS Inf. and Commun. Mag.*, vol. 30, no. 4, pp. 7-15, 2013.
[20] K. Sun and Y. H. Kim, “VM migration with IP mobility management for tactical edge cloud,” *J. KINGComputing*, vol. 15, no. 3, pp. 50-66, Jun. 2019.
[21] H. Jeong, et al., “Shared distributed big-data processing platform model: A study,” *KIISE Trans. Computing Practices*, vol. 22, no. 11, pp. 601-613, Sep. 2016.
[22] K.-W. Kang, et al., “Deployment strategies of cloud computing system for defense infrastructure enhanced with high availability,” *J. KINGComputing*, vol. 15, no. 3, pp. 7-15, Jun. 2019.
[23] J.-B. Kim and J. Park, “Suggestions for defense cloud strategy and development plan,” *J. The Korea Soc. Info. Technol. Policy & Manag.*, vol. 11, no. 2, pp. 1213-1220, Apr. 2019.
[24] J. Koo, et al., “Design of security architecture for the cloud-based korea military command and control system,” *J. KICS*, vol. 45 no. 2, pp. 400-408, Feb. 2020.

진 정 하 (Jungha Jin)

2002년 2월 : 금오공과대학교 전자통신공학과 졸업
2006년 8월 : 건국대학교 정보보안전공 공학석사
2020년 2월 : 건국대학교 정보보안전공 공학박사
2020년 6월~현재 : 고려대학교 정보보호대학원 정보보호연구원 연구교수
<관심분야> Cloud, 사이버 보안, 국방정보시스템
[ORCID:0000-0001-5303-7673]

김 병 준 (Byeongjun Kim)

2008년 2월 : 경북대학교 컴퓨터공학과 졸업
2021년 현재 : 한화시스템 미래정보통신연구소 전문연구원
<관심분야> Cloud 시스템, 사이버 보안, 국방정보시스템
[ORCID:0000-0002-4042-4321]

한 근 희 (Keunhee Han)

1986년 2월 : 서울과학기술대학교 컴퓨터공학과 졸업
1988년 2월 : 한양대학교 정보보호전공 공학석사
2006년 2월 : 고려대학교 정보보호전공 공학박사
2006년~2012년 : 행정안전부, 국가정보자원관리원 사이버안전과장
2013년 11월~2017년 8월 : 고려대학교 정보보호대학원 산학협력중점교수
2017년 9월~2019년 8월 : 건국대학교 소프트웨어학과 교수
2019년 9월~현재 : 고려대학교 정보보호대학원 정보보호연구원 연구교수
<관심분야> Cloud, 사이버보안, 국방정보시스템
[ORCID:0000-0001-6385-0617]