정 보 보 호 학 회 지
제 32 권 제5호, 2022. 10

국방 소프트웨어의 현대화 및 공급망 보안을 위한 DevSecOps 도입 방안 연구

이 승 운*, 류 한 얼**, 홍 수 연**, 김 태 규**

요 약

DevOps는 개발과 운영을 배포 기간을 최소화함과 동시에 안정적인 운영을 목표로 하는 현재 가장 진보된 개발 문화이자 방법론이다. DevOps는 수많은 IT 기업에서 활용되고 있으며, 국방 분야도 마찬가지로 소프트웨어 전력 우위를 선점하기 위하여 DevOps 도입을 고려해왔다. 그러나 사이버 위협의 대응이 부족한 DevOps을 국방 소프트웨어에 적용하기가 쉽지 않다. 이에 미 국방부(Department of Defense, 이하 DoD)는 미래의 사이버 위협으로부터 국방 소프트웨어의 피해를 최소화하고자 DevOps 전 단계에 사이버 보안을 결합한 DevSecOps를 채택하여 개발 및 시범운영 중에 있다. 본 연구에서는 DevOps와 DevSecOps의 개념을 소개하고 국방 소프트웨어 분야의 적용 사례를 살펴본다. 그 중 DoD의 DevSecOps의 구조, 구축 사례, 공급망 보안 방안을 분석하고 이를 바탕으로 우리 군의 DevSecOps 적용 가능성에 대해 논의하고자 한다.

Ⅰ. 서 론

DevOps는 개발과 운영 간의 장벽을 낮추어 소프트웨어의 개발 생산성을 높히고 안정적인 운영을 목표로 하는 문화, 방법론, 기술을 의미한다[1]. 애자일 방법론과 프로세스 자동화를 통해 배포 시간을 단축하고 클라우드 관리 자동화를 통해 안정적인 운영이 가능하다. 신기술 도입의 가속화, 신속한 대응, 비용 절감 등의 장점으로 이미 많은 글로벌 IT기업에서는 DevOps가 보편화되었다. 국방 분야에서도 소프트웨어 전력 우위를 선점하기 위하여 DevOps의 중요성을 인식하고 적용을 추진해가고 있다.

그러나 사이버 보안 문제로 인해 국방 소프트웨어의 DevOps 적용은 쉽지 않았다. 세계는 지금 사이버전이 첨예하게 벌어지고 있고 사이버 공격은 인명피해, 전력손실, 임무 실패, 전쟁의 패배까지 이어진다. 반면 DevOps의 공급망에는 수많은 공개 및 상용 소프트웨어가 활용되어 사이버 공격의 통로가 되기 쉽다. 이에 미 국방부(Department of Defense, 이하 DoD)는 DevOps 전 단계에 사이버 보안을 수용한 DevSecOps를 채택하여 미래의 사이버 위협으로부터 국방 소프트웨어의 피해를 최소화하고자 한다[2].

본 연구에서는 DevOps와 DevSecOps의 개념을 소개하고 국방 소프트웨어 분야의 적용 사례를 살펴본다. 그 중 DoD의 DevSecOps의 주요요소, 구조, 공급망 보안 방안을 분석하고 이를 바탕으로 우리 군의 DevSecOps 적용 가능성에 대해 논의하고자 한다.

Ⅱ. 배 경

2.1. DevOps

DevOps는 기존에 분리되어 있던 개발과 운영을 통합하여 배포 기간을 최소화함과 동시에 안정적인 운영을 목표로 하는 개발문화이자 방법론이며 프로세스, 도구, 표준 등을 아우르는 용어이다. 협업, 소통 중심의 조직문화와 클라우드 인프라를 기반으로 신속하고 적절한 프로세스와 도구을 통해 개발과 운영의 간극을 좁혀 소프트웨어 개발 생명주기를 최소화한다. 즉, DevOps를 적용하면 소프트웨어 개발과 배포에 걸리는 시간이 단축되고 자동화로 인해 프로세스가 간소화된다. 개발부서와 운영부서 간의 지속적인 피드백을

* LIG넥스원 C4I연구소 사이버전연구팀 (선임연구원, seungwoon.lee@lignex1.com)
** LIG넥스원 C4I연구소 사이버전연구팀 (수석연구원, haneul.ryu2@lignex1.com, 수석연구원, suyoun.hong@lignex1.com, 수석연구원, taekyu.kim@lignex1.com)

교환하여 요구사항의 신속한 반영, 품질 향상, 비용절감 등을 달성 할 수 있다.

DevOps는 애자일 방법론이 운영 범위까지 확장된 것으로 볼 수 있다. 애자일 방법론은 전통의 소프트웨어 개발 방법론의 문제들을 해결하기 위해 소프트웨어의 개발단위를 축소하고 프로세스를 반복하는 경량화된 개발 방법론으로 빠른 배포, 빠른 대응, 신기술 도입 등이 가능하게 했다. 그러나 안정적인 운영에 있어 빈번한 배포와 새 기술의 적용은 오히려 단점으로 작용했으며 운영부서의 업무 가중은 부서 간의 갈등을 초래하게 되었다. DevOps에서는 빌드, 테스트, 통합, 배포의 자동화를 통해 해소하고자 했으며 이를 CI/CD(지속적 통합/지속적 전달 및 배포,Continuous Integration/Continuous Delivery and Deployment)라 한다.

이처럼 개발에서 운영까지 모든 공급망에서 자동화가 이루어지므로 이를 지원하는 도구의 도입이 필수하며 이 도구들을 묶어 툴체인(Tool-chain)이라고 부른다. 툴체인에는 빌드, 테스트, 배포용 자동화 도구 뿐만 아니라 협업을 지원하는 프로젝트 관리 도구, 형상관리 도구, 문서화 도구, 안정적 운영을 위한 모니터링, 로깅, 데이터 분석 도구가 포함된다. 게다가 클라우드 네이티브로 운영되는 현대 소프트웨어 체계로 인해 클라우드 플랫폼, 가상화 및 컨테이너 도구, 유지보수 도구 등이 툴체인에 포함되며 핵심적인 역할을 수행한다.

전술하였듯이 DevOps의 공급망에는 수많은 도구들이 연동된다. 상용 및 공개 소프트웨어들이 활용되다 보니 다양한 보안 취약점이 발생할 수 있기에 사이버 공격의 표적이 되어 왔고 그 비율 또한 높아지고 있다. 2022년 Rockstar Games는 협업도구인 Slack의 해킹으로 인해 신작 게임의 정보와 소스코드가 유출된 사례가 있다. 가장 높은 점유율을 차지하고 있는 오픈소스 CI 도구 Jenkins의 취약점은 꾸준히 발견되고 있다. 공급망 대상의 위협은 개발, 배포, 유지보수 모든 측면에서 악영향을 끼친다. DevOps의 개념에 보안이 일부 포함되어 있으나, 점차 DevOps 공급망 보안이 중대한 사항으로 다루어지고 있다.

2.2. DevSecOps

DevSecOps는 DevOps 전 과정에 보안을 통합하는 개념이다. 보통 특정 규모 이상의 기업에는 보안부서를 운영하고 있다. DevSecOps에서는 보안 부서에게도 신속성을 제공하여 프로세스 내의 보안 문제를 즉각적으로 발견하고 개발부서, 운영부서와 피드백을 통해 이를 개선한다. 혹은 개발부서 및 운영부서가 공급망 전체 과정에서 보안을 염두에 둔다.

보안 개선을 위한 도구는 DevOps의 도구들과 마찬가지로 자동화되어야 한다. 보안의 중요성을 인지하고 있음에도 조직문화의 변화를 통해 개선하는 것은 현실적으로 어려운 일이므로 보안을 쉽게 강화하는 방안은 자동화된 도구를 공급망에 적용하는 것이다. 산출물을 대상으로 취약점 탐지 및 관리 도구, 단위시험 도구, 클라우드 인프라 대상 인프라스트럭처 스캔, 컴플라이언스 스캔도구 등을 들 수 있다. 이처럼 다수의 보안 소프트웨어들은 기존 소프트웨어들과도 긴밀하게 운영되어야 한다.

Ⅲ. 국방 소프트웨어와 DevSecOps

3.1. 국방 소프트웨어의 특징

현대전 양상이 네트워크 중심전으로 변화하면서 국방 소프트웨어의 패러다임 역시 변화하고 있다. 임무에 필요한 정보와 명령을 적시적소에 제공하기 위하여 C4I 체계(C4I:지휘(command) 통제(control) 통신(communication) 컴퓨터(computer) 정보(intelligence))가 등장했다. 기존의 국방 소프트웨어의 주를 이루었던 무기체계 분야에서도 소프트웨어 비중이 크게 증가하였으며 C4I체계와의 연동 지원이 필수가 되었다. 군수지원체계와 교육훈련체계 역시 소프트웨어 기반으로 고도화되고 있다. DoD의 합동정보환경(JIE, Joint Information Environment) 구축사례를 미루어 보아 미래에는 소프트웨어/클라우드 기반의 통합된 대규모 체계를 목표로 진화하고 있다.

국방 소프트웨어의 주요 품질 속성으로 신뢰성(Reliability)을 들 수 있다[3]. 국방 소프트웨어의 결함은 생명과 직결된다. 최종 산출물의 결함을 최소화하기 위하여 정적 시험, 동적 시험을 포함하는 소프트웨어 신뢰성 시험이 국방 소프트웨어 개발 프로세스의 필수 절차이다. 이로 인해 국방 소프트웨어는 폭포수 모델, V 모델과 같은 전통적 선형 소프트웨어 개발 프로세스를 진행하게 되며, 짧게는 3-4년, 길게는 10년

이 소요된다.

두번째는 사이버보안(Cyber-security)이다. 사이버 공격을 통해 인프라를 마비시키거나 기밀 정보를 탈취하여 전장의 우위를 점하는 사이버전에서, 국방 소프트웨어는 외부의 위협으로부터 보호되어야만 한다. 현재 대부분의 사이버 보안 프레임워크 (NIST 사이버 보안 프레임워크, ODNI 사이버 위협 프레임워크, NSA/CSS 기술 사이버 위협 프레임워크 v2(NTCTF), MITRE ATT&CK 등)는 주로 최종 산출물을 대상을 하는 공격에 중점을 두고 있다.

세번째로 상호운용성(interoperability)이다. 미래에는 하위 제대에서부터 육해공, 나아가 동맹국 간의 합동작전이 임무 전 영역에서 이루어질 것이다. 따라서 대규모의 엔터프라이즈 환경의 체계 아래 다양한 국방 소프트웨어들이 운영될 것이며 대규모 클라우드 플랫폼 아래 수십억단위의 데이터 교환이 이루어 질 것으로 예상한다.

마지막으로 민첩성(Agility)이다. 급변하는 소프트웨어 생태계에서 기술적 우위를 선점하는 것은 전쟁의 승리에 영향을 미칠 수 있다. 전장 상황에 따라 소프트웨어의 빠른 업데이트가 필요한 경우가 있다. 무기체계의 개발 및 전력화 과정을 의미하는 획득 프로세스(Acquisition process)의 효과적인 개선이 요구된다.

이 네가지 품질속성은 서로 밀접하게 연관되어 있는데 상호보완의 경우도 있으나 상충 관계(Trade-Off)의 경우 역시 존재한다. 예를 들어 신뢰성을 위한 국방 소프트웨어의 긴 프로세스는 민첩성을 보장하기 어렵다. 또한 민첩성을 위해 개선된 공급망에는 보안 문제가 발생할 수 있다.

3.2. DevSecOps 도입

미 국방성은 2018년, 국방 소프트웨어 현대화 전략의 일환으로 Enterprise DevSecOps Initiative을 출범하였다[4,5]. 이에 따르면 DevSecOps의 도입은 신속하고 안전한 방식으로 어플리케이션을 제공할 수 있으며 다음의 장점을 함께 소개했다. 소프트웨어 테스팅 자동화를 통해 동일하거나 더 높은 수준의 신뢰성시험을 진행할 수 있다[6]. 기획부터 운영까지 사이버 보안 기능 및 정책을 도입하고 시행할 수 있다. 애자일 방법론에 맞추어 개발 과정과 검증 및 인증 전 일정이 단축된다. 클라우드 기반의 컨테이너 환경에서 동작하므로 원활한 이식성이 보장된다. 즉 국방 소프트웨어의 주요 품질 속성을 보장하는 해결책이 될 수 있음을 의미한다. 단, 소프트웨어 현대화 전략 문서에 따르면 품질속성 간의 우선순위을 설정해야 하는 원칙이 여전히 존재하기에 품질속성 간의 상충관계는 여전히 고려해야 할 사항이다[4].

3.3 도입 사례

3.3.1 미국

DoD는 방산기업 및 글로벌 빅테크 기업 등과 긴밀한 협력관계를 구축하고 DevSecOps을 실험적으로 도입해오고 있으며 일부에서는 프로세스 단축의 효과를 확인하였다.

보도자료에 따르면 록히드 마틴(Lockheed Martin)은 DevSecOps 프로세스를 기반으로 미공군 및 미사일 방어 사령부와 협력하여 F-35, U2와 다중도메인 연결 시험을 완료하였고 F-35A 및 F-16에 자동 지상충돌 방지 체계 통합하였다. 노스럽그루먼(Northrop Grumman)은 미공군의 DevSecOps 플랫폼 지원하는 파트너십을 맺고 차세대 고급 사이버 도구를 개발하고 있으며 차세대 미사일 개량사업인 GBSD(Ground Based Strategic Deterrent)에도 DevSecOps를 적용하고 있다. 레이시온(Raytheon)은 미공군의 공중/우주작전 센터 무기 체계 (AOC WS, Air and Space Operations Center Weapon Systems)에 DevSecOps를 활용하고 있다.

DoD 문서에 따르면 특정 벤더의 종속성을 최소화하기 위해 DevSecOps 클라우드 플랫폼의 호환성을 열어두고 있다. 반면 실제 활용될 국방 클라우드 플랫폼의 운영 규모가 방대할 것으로 예상되어 민간 빅테크 대기업 간의 경쟁이 심화되고 있는 상황이다. 2022년 10월 기준을 기준으로 업체 선정 과정 중이며 참여기업은 아마존(Amazon), 마이크로소프트(Microsoft), 구글(Google), 오라클(Oracle)로 알려져 있다. 멀티 클라우드 벤더로 수주가 예상돼 종속성 방지와 운영 탄력성에 이점이 있을 것으로 판단된다.

상용 클라우드 플랫폼 1위 기업인 아마존의 AWS(Amazon Web Service)는 이미 널리 활용되고 있어 DoD에서도 AWS에 대한 DevSecOps 레퍼런스 디자인 문서를 배포하였다. 마이크로소프트의 Azure

는 미 해군 소프트웨어 공장의 클라우드 플랫폼으로 선정되어 운영되고 있다. 오라클은 미 공군의 ABMS(Advanced Battle Management System)의 클라우드 플랫폼 제공자로 선정되었다. 레드햇(RedHat)은 Compile to Combat in 24 Hours (C2C24) 사업에 DevSecOps를 적용하였으며, 자사 제품인 OpenShift, Ansible 등을 공군 DevSecOps 프로세스에 적용하였다.

3.3.2 영국

영국은 D2S(Defense DevSecOps Service)를 통해 업계 모범사례와 공급망을 제공하고 있다. D2S는 컨테이너화된 애플리케이션을 구축하고 확장하기 위한 안전한 하이브리드 클라우드 기반을 제공하는 Red Hat OpenShift를 활용한다. D2S는 영국의 소프트웨어 개발 가속화 프로젝트인 PREDA(Platform for Rapid Exploitation of Digital Applications)에서 애자일 소프트웨어 개발을 위한 수단으로 제공된다.

DevSecOps의 보안이 중시되는 철학을 달성하기 위하여 플랫폼의 모든 애플리케이션에 대해 완전한 SbD(Secure by Design) 방법론을 제안하고 구현을 목표라 한다. SbD 접근 방식은 소프트웨어 제공 수명 주기 전반에 걸쳐 위험 관리 프레임워크를 따르고 지속적인 모니터링과 보안을 보장한다.

3.3.3 NATO

NATO (북대서양 조약 기구, North Atlantic Treaty Organization)는 연합작전의 전술엣지에서 클라우드 컴퓨팅의 활용가능성을 조사하는 IST-168 연구 태스크 그룹을 구성하였다. 이 연구팀은 연합국간의 쿠버네티스 클러스터 연결을 위한 상호운용성을 주로 연구해왔다. 또한 DevSecOps의 모범 사례를 반영하기 위하여 NATO 소프트웨어 공장을 마이크로소프트의 Azure를 활용해 구축하였다.

Ⅳ. DoD DevSecOps

DevOps의 3요소는 사람과 문화, 기술, 프로세스로 꼽는다. 본 장에서는 그 중 DoD DevSecOps의 기술 및 플랫폼, 프로세스를 알아본다. 기술된 내용은 DoD 공식 발행문서를 참조하였다.

4.1. 핵심 기술요소

DoD DevSecOps의 핵심 기술 요소는 DevOps의 철학, 클라우드/컨테이너 기술, 보안 중심, 국방 분야의 요구사항 등을 반영하고 있다.

- **추상화** - 국방 소프트웨어가 특정 벤더의 종속되는 것을 막기 위해 개방형 표준을 따르는 쿠버네티스 및 컨테이너를 활용한다.
- **IaC(Infrastructure as Code)** - 구성, 네트워킹 등 모든 인프라는 코드 형태로 작성되며 공급망 파이프라인이 자동으로 인스턴스화된다.
- **CI/CD 파이프라인** - DevSecOps의 모든 도구들은 컨테이너화고 IaC에 의해 자동으로 공급망이 구축된다.
- **강화된 컨테이너** - 소프트웨어들은 컨테이너화되는 과정에서 스캐닝, 취약점 분석, 보완, 서명 절차를 갖는다.
- **전 단계 보안 (Baked-In Security)** - 개발 초기 부터 정적/동적 분석, 컨테이너 스캔, BOM(Bill of Materials) 확인 등의 보안행위가 의무화된다.
- **지속적인 모니터링** - 클라우드 설계의 사이드카 패턴(Side Car Pattern)을 활용하여 컨테이너, 함수 수준의 보안, 중앙 집중 식 로깅 및 텔레메트리(원격 측정), 자동경고, 위협행위 탐지, 취약점 스캐닝 등을 수행한다.
- **Chaos engineering** - 예상치 못한 장애 발생에도 컨테이너는 자동으로 중지, 재시작, 자동확장(auto-scale) 등을 수행할 수 있다.

4.2. DevSecOps 플랫폼 구조

DevSecOps의 플랫폼 구조는 그림 1과 같이 계층 구조로 설명할 수 있다. DevSecOps의 공급망을 구성하는 가장 아래의 계층은 인프라 계층이다. 퍼블릭 클라우드 환경을 의미하며 국방 특성상 온프레미스, 분리망, 임베디드 환경도 제공할 수 있어야 한다. 상위는 플랫폼 계층으로 컨테이너와 컨테이너 관리 기능을 의미한다. DoD는 벤더 종속성을 최소화하고자 오픈소스 컨테이너 오케스트레이션 기술인 쿠버네티스에 위임하였다. CI/CD 계층에서는 DoD로부터 인증된 자동

〔그림 1〕 DevSecOps 플랫폼 구조

화 도구들을 컨테이너화하여 제공한다. 제공된 컨테이너들로 DevSecOps 공급망 파이프라인을 구성한다. 다음은 서비스 메시 계층이다. 이 DevSecOps로 인해 산출되는 소프트웨어는 소프트웨어 현대화에 따라 마이크로서비스의 집합으로 간주한다. 서비스 메시는 마이크로서비스 간 통신을 제어하고 지원하는데 개발 단계에서부터 운영까지의 사이버 보안을 담당하는 마이크로서비스가 함께 동작한다. 마지막 계층은 응용계층으로 DevSecOps 플랫폼의 자동화 프로세스를 통해 부가적인 업무를 최소화하여 개발부서가 소프트웨어 개발에 집중할 수 있도록 한다.

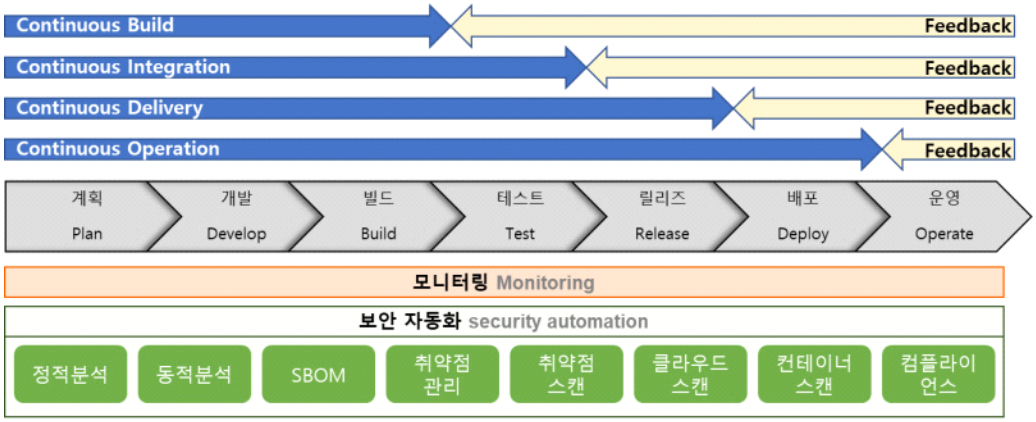
4.3. DevSecOps 프로세스

그림 2과 같이 DoD DevSecOps의 프로세스는 전통적인 소프트웨어 개발 프로세스와 유사하게 계획(Plan), 개발(Develop), 빌드(Build), 테스트(Test), 릴리즈(Release), 배포(Deploy), 운영(Operate), 모니터링(Monitoring)을 포함한다. 이 과정들의 자동화를 위해 다양한 공개 및 상용 소프트웨어가 컨테이너화되어 지원한다. 보안은 DevSecOps의 철학에 따라 전 과정에서 관여해야 한다. 취약점 스캔, 테스팅, 검증 등 보안 자동화가 과정마다 이루어지며, 과정 간에도 지속적인 위협을 특정해내기 위하여 정적분석, 동적분석, BOM 확인, 컨테이너 보안 스캐닝 등의 자동화 과정이 동반되어야 한다. DevSecOps 엔지니어를 위한 대시보드와 대응방안 역시 검토되어야 한다.

4.4. DevSecOps의 공급망 보안

Reffett 등은 DevSecOps의 공급망 보안 위협 대상을 클라우드 인프라, 플랫폼(컨테이너), 소프트웨어 공장, 미션시스템(소프트웨어 산출물)로 나누고, 일반적이지만 근본적인 개선방안을 제시하였다[7].

먼저 클라우드 인프라가 공격의 대상이 될 수 있음을 인지해야 한다. AMI (Amazon Machine Image), 리눅스 커널, 하이퍼바이저 대상의 시스템 공격, SPOF(Single Point of Failure), DDoS(Distributed Denial of Service)와 같은 기반망 공격은 클라우드 전체를 무력화시킬 수 있다. 따라서 가용성을 보장하는 대응 방안 계획과 주기적인 훈련이 필요하다. 클라우드는 모니터링을 통해 보안 가시성이 확보되어야 하며 이 모니터링 인프라 역시 사이버공격의 대상이 될 수 있음을 인지해야 한다. 쿠버네티스와 같은 컨테이너 플랫폼은 다수의 상용 및 공개 응용플랫폼, 라이브러



〔그림 2〕 DevSecOps 프로세스

리, 컨테이너로 구성된다. 공급망 구축 시 필요한 모든 구성요소를 숙지하고 필요하지 않은 요소는 제거해야 한다. 소프트웨어 공장에서는 인증된 이미지만을 사용하고 취약점 스캐닝 도구를 통해 컨테이너 내부의 패키지를 관리한다. 개발에 사용할 라이브러리의 확인 절차 또한 필요하다. 가능하다면 다수가 사용한 검증된 라이브러리를 사용하며 타이포스쿼팅(Typo-Squating) 공격을 방지하기 위해 오탈자에 신경을 써야 한다.

종합하자면 공급망을 구성하는 모든 소프트웨어, 도구, 벤더를 엄밀히 확인해야 한다. 공급망 운영중에는 모니터링 및 제어가 동반되어야 하며 능동적인 사전보안과 신속한 대응을 갖춰야 한다.

Ⅴ. 우리 군 적용방안

DevOps의 역사는 짧지만 이미 많은 IT 기업에서 이를 도입하거나 관련된 솔루션을 출시하고 있다. 반면 아직 군에서는 DevOps, DevSecOps의 적극적으로 이루어지지 않는 것으로 보인다. 본 장에서는 DevSecOps의 3요소인 기술, 프로세스, 사람과 문화를 바탕으로 우리 군의 적용방안에 대해 논의한다.

DevSecOps의 기반기술인 클라우드의 필요성은 이미 우리 군에서도 인식하고 있으며 일부는 이미 운영중에 있다[8]. 클라우드 보안 요구사항을 반영하기 위한 연구 및 사업이 산학연에서 다수 수행중이다[9,10,11]. 또한 우리 군은 소프트웨어를 안전하게 관리하기 위하여 RMF A&A(Risk Management Framework Assessment & Authorization) 표준에 따라 구매 관리 절차를 수행한다[12]. 이를 미루어 볼 때 클라우드, 보안 분야의 세부 기술들의 연구는 활발하게 진행중임을 알 수 있다. 단, 현재 기술을 선도하는 테크기업과 실제 개발을 수행하는 방위산업체, 그리고 운영 주체인 군 간의 활발한 기술적 교류와 이를 지원하는 법 제도의 개선이 필요할 것이다.

두 번째로 소프트웨어 전력화까지의 오랜 시간이 소요되는 기존 프로세스의 문제점을 극복할 필요가 있다. DevOps의 근간이 되는 애자일 방법론과 스크럼(Scrum)을 국방 전장관리체계 연구개발 사업과 유지보수 사업에 적용하는 방안을 연구한 사례가 있다[13,14]. 그러나 일반 사기업에서도 애자일 방법론의 적용이 어려운 일이다. 특히 한국기업의 보수적 특성과 애자일 방법론의 자율성 사이의 많은 충돌이 발생했다. 따라서 국내외 극복 사례를 통해 점진적으로 국방 프로세스에 적용하는 방안을 모색해야 할 것이다[15].

마지막으로 DevSecOps 인력양성이 필요하다. 군에서도 IT 인재양성을 위해 큰 노력을 펼치고 있으며 현재 AI, 코딩 등의 IT 기술을 대상으로 하는 인재양성이 주를 이룬다. 동시에 DevSecOps와 같은 소프트웨어 공학의 소양도 함께 교육되어야 할 것이다.

DevSecOps는 아직 도입기이며 여전히 많은 비판과 보완 사항이 존재한다. 따라서 해외 성공사례를 쫓아 DoD의 DevSecOps를 그대로 도입해선 안 된다. 소프트웨어 개발 방법론은 상황에 맞게 변이 가능하다.우리 군의 상황, 개발 문화,체계에 적합한 테일러링 된 DevSecOps를 도출하는 연구가 필요할 것이다.

Ⅵ. 결 론

미국 국방부는 DevSecOps를 도입하여 국방 소프트웨어 전력화에 소요되는 시간을 줄임과 동시에 사이버 위협에 대응하고자 했다. 이에 본 연구에서는 DevSecOps의 적용 사례와 미국 DoD의 DevSecOps의 구조를 살펴보고, 우리 군의 적용가능성에 논의하였다.

DoD DevSecOps는 계속 진화하고 있다. 향후에는 DoD DevSecOps의 개선사항 등을 추가로 분석하고 무기체계 소프트웨어 개발 및 관리 지침을 참조하여 보다 현실적인 우리 군 적용 방안에 대해 연구할 것이다.

참 고 문 헌

[1] 전인석, “보안을 고려한 무중단 환경에서 개발운영 조직 통합관리(DevOps)”, *정보보호학회지*, 25(1) pp.47-52, 2015.

[2] *DoD Enterprise DevSecOps Fundamentals*, Ver.2 March 2021.

[3] 류지선, 송치훈, 권순모, 박병훈, 오진우, "무기체계 최초양산품 소프트웨어 품질보증 프로세스 연구." *한국산학기술학회논문지,* 22(1), pp. 285-293. 2021

[4] *Department of Defense Software Modernization*

Strategy, Ver.1 November 2021.

[5] A. Miller, R. Giachetti, D. Van Bossuyt, “Challenges of Adopting DevOps for Combat Systems Development Environment,” *Defense Acquisition Research Journal*. 29. 22-48, 2022

[6] M. Bate, E. I. Oviedo, "Software Reliability in a DevOps Continuous Integration Environment," *in proceedings of 2021 Annual Reliability and Maintainability Symposium (RAMS)*, November 2021

[7] A. Reffett, R. Luaghlin, “Software Supply Chain Risks to DevSecOps Programs,” Webinar, 2021

[8] 박준규, 이상훈, 박기웅, “국방 지휘통제체계의 클라우드 도입 방안,” *디지털문화아카이브지* 2(1), April 2019.

[9] 장월수, 최중영, 임종인, “국방 클라우드 컴퓨팅 도입에 관한 보안체계 연구,” *한국정보보호학회논문지, 22*(3), pp. 645-654, June 2012

[10] 구자훈, 김영갑, 이상훈, “클라우드 기반 미래 한국군 지휘통제체계 보안 아키텍처 설계,” *한국통신학회논문지*,45(2), pp. 400-408, 2020

[11] 진정하, 김병준, 한근희 “클라우드 기반 국방 정보시스템 구축에서의 정보보호 적용 방안 연구,” *한국통신학회논문지*, 46(9), 2021

[12] 조광수, 김승주, “무기체계 개발을 위한 RMF A&A의 실증에 관한 연구,” *정보보호학회논문지* 31(4), pp. 817-839, 2021

[13] 윤성현, 임규건, “국방 전장관리정보체계 연구개발 사업의 애자일 적용 방안,” *한국IT서비스학회지* 20(1), pp. 41-54, 2021

[14] 최은희, “국방정보체계 유지보수 사업에서의 스크럼 개발방법론 적용 효과 연구,” *선진국방연구* 1(1),pp. 87-108, 2018

[15] 심승배, “국방 R&D 프로세스 진단 및 혁신 방안,” *국방이슈브리핑시리즈* 2019-16, 2019

〈저자소개〉

이 승 운 (Seungwoon Lee)
정회원
2021년 2월 : 아주대학교 컴퓨터공학 박사
2021년 1월~현재 : LIG넥스원 C4I연구소 사이버전연구팀 선임연구원
<관심분야> 사이버전, 소프트웨어공학

류 한 얼 (Haneul Ryu)
2011년 2월 : 한국항공대학교 컴퓨터공학 석사
2011년 1월~현재 : LIG넥스원 C4I연구소 사이버전연구팀 수석연구원
<관심분야> 사이버전, 시스템 및 네트워크 가상화

홍 수 연 (Suyoun Hong)
2013년 2월 : KAIST 전기 및 전자공학 박사
2013년 2월~현재 : LIG넥스원 C4I연구소 사이버전연구팀 수석연구원
<관심분야> 사이버전, 소프트웨어공학

김 태 규 (Taekyu Kim)
정회원
2008년 5월 : University of Arizona, 컴퓨터공학 박사
2010년 2월~현재 : LIG넥스원 C4I연구소 사이버전연구팀 수석연구원
<관심분야> 사이버전자전, 무기체계 사이버보안