https://doi.org/10.33778/kcsa.2021.21.4.031

# AI백신체계 연구개발 제품의 국방분야 실증 프로세스 개선 연구★

윤 석 준*, 김 종 현**, 이 상 민**, 강 지 원***


## 요 약

국방 무기체계 연구개발 시 기술적, 운용적 측면의 평가는 군 자체 시험평가제도를 두고 발전해 왔고 이를 위한 조직과 절차가 확립되어 시행 중이다. 그러나, 최근 민간분야 정보통신기술 발전이 고도화되면서 민수 기술 연구개발 과정에서 개발이 완전히 끝나기 전에 국방 분야에 필요한 기술의 운용성이나 적합성을 확인함으로써 연구개발의 합목적성과 실용성을 높이는 방법으로 현장 시범적용을 할 필요가 발생하는 경우가 있다. 본 논문은 과학기술정보통신부 주관, 최신 AI백신체계 연구개발 시제품을 국방영역에 실증시험을 하기 위한 프로세스와 관련한 사항을 조사·분석하고 기존의 군 정보체계 시험평가 절차의 개선한 실증방안을 제안한다. 또한, 국방 환경의 특수성·보안성 하에서 보안기술 시제품을 실증을 수행하기 위한 프로세스의 개선과 현실적 적용 가능한 실증방안을 제시하고자 한다.


# A Study on Improving the Demonstration Process in the Defense Area with AI Anti-virus System R&D Products

Sukjoon Yoon*, Jonghyun Kim**, Sang-min Lee**, Jiwon Kang***


## ABSTRACT

In the R&D of the Defense Weapon System, the evaluation of technical and operational aspects has been developed with the military's own test evaluation system, and organizations and procedures have been established and implemented. However, with the recent advancement of information and communication technology in the private sector, it is often necessary to test-apply it to the field by enhancing the operability and suitability of technologies required for defense before development is complete. This paper investigates and analyzes the process for conducing empirical tests on the latest AI vaccine system R&D prototype organized by the Ministry of Science and ICT which proposes an improved demonstration plan for the existing military information system test evaluation procedure. In addition, under the specificity and security of the defense environment, we would like to present a practical demonstration plan and the improvement of the process for demonstrating the security technology prototype.


**Key words : AI Vaccine, Demonstration, Demonstration Test, Technology Demonstration, Security Measure**

접수일(2021년 10월 08일), 수정일(2021년 10월 28일), 게재확정일(2021년 10월 30일)

★ 이 논문은 2021년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임. (No.2019-0-00026, 지능화된 악성코드 위협으로부터 ICT 인프라 보호)

* 세종대학교 사이버전연구소

** 한국전자통신연구원 네트워크시스템보안연구실

*** 세종대학교 컴퓨터공학과 (교신저자)

# 1. 서 론

최근 국방 및 국방산업 분야에 대한 사이버공격은 최신 악성코드를 이용하여 점차 악성화·지능화되고 있다. 기존 상용 백신 솔루션이 가지고 있는 신·변종 악성코드의 실시간 처리가 곤란한 경우가 발생하고 여러 보안프로그램의 차이로 인한 시스템 자원 부족, 이기종 보안프로그램 간 호환성 부족의 문제 등 여러 한계점이 있다[1]. 한편, 국방 분야에 4차 산업혁명 요소기술의 적용 확대에 따라 국방 ICT 환경이 변화되고 있는 가운데 이러한 환경에서 적용을 위한 다수준·다계층 위협 대응을 위한 클라우드 기반의 인공지능(AI) 백신 기술의 개발을 활용하려는 요구가 증대하고 있다.

이러한 시점에서 연구소나 기업체에서 연구 개발된 AI백신 기술을 단순히 연구로 그치지 않고 제품화되고 상용화될 수 있도록 연구개발 후, 실증시험을 통해 주요기능, 운용성 및 적합성을 평가하여 그 성능과 효과를 입증하는 것은 매우 중요하다. 이를 통해, 수요기관이 요구하는 AI백신 체계에 더욱 근접할 수 있고 개발된 원천기술의 적용성을 높임으로써 그 활용성을 보장할 수 있다. 특히, 국방 분야는 조직의 특수성과 임무의 보안성으로 인해 타 부처 연구개발 시제품을 시범 적용하여 실증하기 쉽지 않고 절차도 분명하지 않은 실정이다.

본 논문에서는 타부처 또는 민간 주도로 사이버 보안(정보보호) 신기술 연구개발 시 국방 분야에서 테스트베드(Test-bed)로서 실증 시험하기 위한 정책을 살펴보고 국방분야 실증 요구사항을 반영하여 실증시험을 위한 프로세스를 제안하고자 한다. 또한, 국방분야 실증시험을 위한 계획 수립과 실증시험 시행 절차를 개선하고 실증시험 시 수반되는 보안대책 검토사항을 함께 제안하고자 한다.

# 2. 관련 연구

## 2.1 AI백신체계 연구개발 기술

국방부는 지능화, 고도화되고 있는 신종 사이버 공격에 대비하기 위해 국방 네트워크 환경에 특화되며, 사이버 공격 패턴을 실시간 분석하고 능동적으로 대응할 수 있는 인공지능 백신 체계 확보를 추진하고자 요구사항을 제시하였다. 이에 따라 과학기술정보통신부 예산 지원을 받아 한국전자통신연구원(ETRI)은 기존의 패턴 기반 백신 엔진에서 탐지하지 못하던 수많은 변종·신종 악성코드를 머신러닝 및 딥러닝 기술을 활용한 AI 기반 악성코드를 분석·탐지하는 기술 연구를 수행하였다. 이 과정에서 국방부는 기존의 타 부처(과기정통부) 산하의 ETRI가 주도하는 AI백신 체계를 국방 분야에 적용하기 위한 국방AI백신체계 협의체를 구성하였다.

국방부와 ETRI가 추구하고자 하는 AI백신 체계의 기본 요구사항은 다음과 같다.

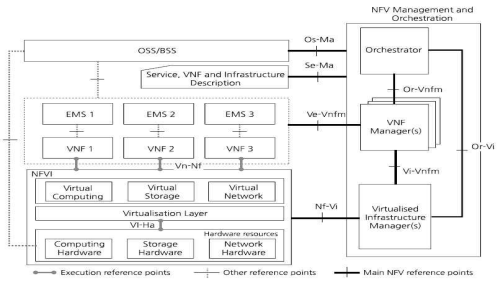
- 현 국방 백신 체계와 복합 운용할 수 있어야 하고
- 국방ICT 환경에서 AI기반 악성코드 분석 및 클라우드 기반의 백신 체계 서비스를 제공하며,
- AI백신 체계 구축 완료 후 추가 운용유지 비용, 조직 변화가 최소화되어야 한다.

AI백신 체계의 핵심은 경량 AI 에이전트를 개발하여, 단말처리의 부하를 줄이고 클라우드 환경에서 개방형 API를 통해 다중 백신 및 AI백신 엔진의 구동을 자동화함으로써 AI기반의 악성코드 분석기술을 적용할 것으로 예상이 된다.

이와 같은 AI백신 체계 개발을 위해 다음과 같은 기술들이 검토되었다.

- 클라우드 백신 오케스트레이션 기술

AI 백신 체계는 VNF(Virtual Network Functions), NFV(Network Function Virtualization) 인프라, 그리고 (그림 1)의 NFV 관리 및 오케스트레이션 모듈로 구성된다.




(그림 1) NFV 참조 기능구조

• 국내 백신 회사들의 AI 악성코드 분석기술 고려

- 안랩의 ASD(AhnLab Smart Defense)기술

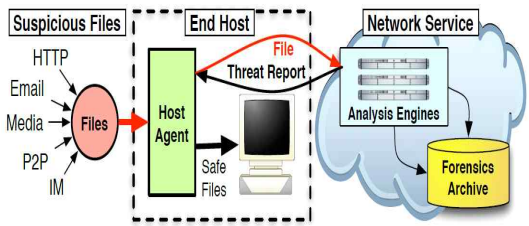
- 이스트시큐리티의 딥러닝 악성코드 위협 대응 솔루션인 Threat Inside

- 이글루시큐리티의 머신러닝 기반 SPiDER TM AI Edition

- 세인트시큐리티의 클라우드 기반 악성코드 자동 분석 플랫폼, malwares.com의 위협정보에 대한 학습형 실시간 대응 AI 백신, MAX 등이 있다.

• 경량 인공지능 백신 에이전트 기술

자체 검색을 수행 할 컴퓨터에 최소한의 로드를 부여하는 (그림 2)의 CloudAV(cloud antivirus) 기술로 Oberheide와 같이 경량 에이전트 솔루션을 고려하고 있다.




(그림 2) Architectural approach for in-cloud file analysis service

• 클라우드 기반 다중 인공지능 백신 표준 분석 플랫폼

VirusTotal 서비스를 통해서 알 수 있듯이, 백신사들은 모두 고유의 악성코드 네이밍 체계를 갖고 있으며, 다양한 백신이 존재하는 환경에서 하나의 악성코드 네이밍을 갖는 것은 매우 어려운 일이다. 이러한 네이밍 체계를 위한 방법으로 AV Class가 활용되고 있다. 즉, 악성코드로 정의하기 위한 공통의 분류방법이 요구되며 이를 위한 솔루션으로 활용될 수 있다.

• 악성코드 및 위협정보에 대한 국내·외 표준화

- 악성코드 및 사이버 위협정보 공유 관련 기술 : 국내 표준은 한국정보통신기술협회(TTA), 한국전자통신연구원(ETRI). 한국인터넷진흥원(KISA)을 중심으로 악성코드 및 사이버 위협정보 공유와 관련된 표준화를 수행한다.

- 국제 사이버 위협정보의 표현과 교환을 위한 표준화 : 국제 멀웨어 시험표준 기구, AMTSO (Anti-Malware Testing Standards Organization)는 악성코드 탐지 및 대응 기술에 대한 테스트 방법을 두고 표준을 주도하는 기관으로, 바이러스 보안업체와 보안제품 평가기관 만이 회원으로 가입할 수 있다.(카스퍼스키, 맥아피, 안랩, 세인트시큐리티 등 가입.)

<표 1>은 AI 백신의 4가지 핵심기술 개발을 요약한 것이다.

<표 1> 기술동향과 핵심기술 개발 요약

| AI 악성코드 분석 | 경량 AI 에이전트 | 다중 AI 분석플랫폼 | AI 악성코드 분석 국제표준 |
|---|---|---|---|
| · 전문 인력의 판단에 의존하는 신·변종 악성코드 분석<br>· 기존 시그너처 기반의 제한적 탐지<br>· Fileless 악성코드에 대응 기술 부재<br>· 단일 백신 진단 기반 악성 여부 진단 방법 단조로움 | · 다기능 제공으로 단말 시스템 성능 저하 원인 제공<br>· 대용량 백신 패턴 DB 탑재<br>· 단일 백신 업체에 종속적<br>· 리눅스 전용 악성코드 분석 및 백신 솔루션 부족 | · 악성코드 진단에 따른 부하 대응에 어려움<br>· 대용량 Unknown 파일에 대한 분석가 기반 수동적 대응<br>· 단일 백신 중심의 악성코드 탐지 성능 한계<br>· AI기반 악성코드 분석시스템의 치료 기능 부재 | · 이기종 상용백신 간의 호환성 문제 상존<br>· 다중 AI 백신 기반의 악성코드 분석 기술의 표준화 부재 |

## 2.2. 무기체계 연구개발시 시험평가

무기체계의 시험평가 종류에는 획득방법에 따라 구매(실물평가, 자료평가), 연구개발(개발시험평가;DT, 운용시험평가;OT), 핵심기술시험평가(DT/OT), 민군기술협력사업(무기체계개발, 기술개발, 국산화)로 나뉘며 이밖에도 ACTD(신개념기술시범사업) 군사적 실용성 평가가 있다.

일반적인 무기체계의 시험평가 과정을 살펴보면 시험평가의 목적을 기술적 개발목표의 충족 여부를 확인하는 DT(소요군 주관하에 기품원이 수행 및 기술지원)와 작전환경 또는 동일한 조건에서 주요 군사요구도 충족을 확인하는 OT(각 군의 운용시험평가기관)로 구분한다. 이 두 가지 시험평가 모두 국방부 전력정책관실에 제출되는 TEMP(시험평가기본계획서)에 의하여 합참에서 확정하도록 규정하고 있다.

• 구매 시 시험평가절차를 살펴보면 방사청이 무기체계 구매 시 국내·국외를 막론하고 합참에 구매시험평가를 요청한다. 합참은 방사청에 제안요청서에 포함할 통합시험평가에 필요한 자료 또는 기술검토를

요청할 수 있고 방사청은 업체로부터 받은 자료들을 합참 및 소요군에 제공한다. 구매 시 시험평가는 실물에 의한 시험평가 수행을 원칙으로 하되 개발 중으로 시제품이 없는 경우, 국내에서 현재 운용 중인 무기체계를 일부 개조하여 구매하는 경우, 국내외에서 운용 중인 무기체계를 함정 또는 항공기 등에 복합무기체계와 통합하기 위해 구매하는 경우 등에 한해 자료에 의한 시험평가를 시행할 수 있다.

• DT는 업체에서 작성한 개발시험평가 계획을 기초로 기품원이 소요군에 계획을 통보하며 소요군은 이에 참여할 수 있다. 시험평가계획서에는 평가 개요에서 대상장비, 수량, 방법, 기간, 장소 항목, 기준, 평가단, 시험장 및 시험장비 등 특성을 측정할 수 있는 환경을 정의하며 결과는 군사요구도(목표성능) 충족·미달로 판정한다.

• OT는 개발간 환경시험을 통한 평가로부터 1 계절 평가, 혹한기, 혹서기를 고려한 3계절 평가까지 적절한 환경과 시기를 적용하여 실시하고 사업 추진 간에 TEMP에 근거하여 ROC(군사요구도)의 변경 또는 OE(운용환경) 변화를 고려, 운용시험 평가방법을 검토하도록 제도화되어 있다. 평가내용은 개발시험평가의 내용과 유사하나 전력화 지원요소와 군운용적합성 평가가 추가되며 결과는 군사용 적합·부적합으로 판정한다. 시험평가에 대한 비용은 기술개발업체에서 개발비용에 포함하여 개발비용을 산출하므로 업체가 부담하도록 규정한다. 또한, 정보통신 기능이 내장된 무기체계에 대해서는 무기체계 운용시험 평가계획 수립 시 상호운용성 관련 내용을 포함하여 시험하도록 정하고 있고 그 결과를 정보화 기획관실에 통보함으로써 기능을 확인한다.

• 핵심기술연구개발 시험평가는 응용연구단계에서 과제가 종결되고 시제품이 제작된 경우 실시하는 시험평가로 DT를 실시하고 적용 무기체계의 유무에 따라 OT를 실시할 수 있다. 평가내용은 DT와 유사하나 개발 직후의 기술임을 감안, 기준미달항목 및 보완계획 항목이 포함되어 있다.

• ACTD사업에 대한 군사적 실용성 평가는 합참이 방사청, 기품원 등 관련 기관의 의견을 참조한 실용성 평가계획을 확정하면 소요군은 이를 근거로 시험평가를 실시하며 결과는 기준충족·기준미달로 판정한다. ACTD사업이 보완절차를 수행한 경우 연구개발 시험평가절차를 적용할 수 있으며 중복되는 시험은 군사적 실용성 평가 결과를 활용할 수 있다[8].

• 민군기술 협력 사업에 대한 시험평가는 주관연구기관이 연구개발의 결과를 시험 평가할 필요가 있다고 판단할 때 국과연에 요청한 과제를 대상으로 한다. 시험 요청절차는 국과연에서 방사청으로 요청하면 방사청에서 검토 후 군적용 시험평가 필요성이 인정될 시 합참에 시험평가를 요청하고 이후 절차는 합참의 시험평가 절차와 동일하다. 다만, OT 결과를 판정함에 있어 사업 특성상 “개발 중 후속 단계전환” 또는 “후속 사업으로 시제품을 개발”하도록 사업을 추진하기 위해 “잠정”이라는 용어를 추가로 사용하여 판정이 가능하다. 민군기술협력사업은 민군협력구도로 인해 부서 업무분장이 복잡하다. 또한, 시험평가에 대한 비용 산정도 요청자 부담이 원칙이다.

### 2.3. 정보체계 연구개발시 시험평가(정부 R&D)

국방정보통신구축사업에서 시험평가는 무기체계 시험평가와 동일하게 DT와 OT로 구분, 실시한다. 만일, 무기체계에 포함된 정보체계사업의 경우에는 그 결과를 소요 군 및 기관이 인수받아 검수 단계에서 인수시험평가를 추가하여 실시한다. 통합 실시원칙도 동일하며 사업의 특성에 따라 분리 시에는 집행기관과 소요제기기관이 협의하여 결정한다. 시험평가는 소요제기기관 책임하에, 시험평가단을 구성하여 집행기관의 지원을 받아 수행하며, 소요제기기관, 시험평가단, 집행기관 등과 협의하여 추진한다. 단, 개발시험평가를 분리하여 수행하는 경우 집행기관의 책임하에 시험평가단을 구성하여 수행한다.

• 상용정보통신제품 도입 시에는 제품 선정을 위한 평가와 검수(인수시험)로 시험평가를 대체한다. 다만, 정보시스템 구축 사업의 일부로 도입하는 상용정보통신제품은 개발된 업무응용 소프트웨어에 통합하여 시험평가를 할 수 있다.

• 소요제기기관은 집행기관의 지원을 받아 시험평가계획을 수립하고, 상호운용성 및 정보보호 시험평가에 대해서 상호운용성 관리 및 별도의 훈령을 준용하

여 평가계획을 작성하고 해당 분야 업무를 위임받은 기관 또는 전문기관에 시험평가를 의뢰한다.

• 평가 항목은 소프트웨어의 품질(기능성, 신뢰성, 사용성, 효율성, 유지 보수성, 이식성), 성능(가용성, 부하 테스트 등), 정보시스템 통합, 상호운용성 및 연동 요구사항, 정보보호대책이 핵심이며 기타, 문서화 내역, 군 운용 적합성, 상용정보통신제품 요구규격. 초기자료 구축 및 이관, 국제적으로 또는 국내 표준으로 정한 세부적인 절차, 성과지표의 측정에 필요한 데이터의 자동 수집여부 등 소프트웨어 산업 진흥법이나, 국가계약법 저촉 여부를 확인하고 있다. 시험평가 결과는 군사용 적합·부적합으로 판정하며 전력화 계획을 포함, 정보화 기획관실에 최종 보고한다.

• 한편, 타 부처 R&D 사업에 대한 군 적합성 평가 및 활용 방법으로 ① 소요제기기관에서 체계 검수 후 시범사업일 경우 사업 성과물을 대상으로 군 적합성을 평가하고, 결과를 국본(정보화 기획관실)에 보고하고 ② 군 적합성 평가 시 국과연, 국방연 및 외부 자문인력을 포함한 평가팀을 구성하여, 체계에 대한 안전성, 신뢰성, 상호운용성, 적용 가능성 등을 평가하고 향후 발전 과제 등을 제시하며 ③ 국본(정보화 기획관실)은 사업 결과를 각 군 및 기관에 전파하고, 각 군 및 기관은 국방정보화기본계획에 우선적으로 반영하도록 하고, 사업 완료 후에는 필요시 관련 부처로부터 소유권 양도문서 접수 후 자산등록 관리하도록 하고 있다.

• 국방정보화업무훈령(국방부훈령제2436호, 2020. 6. 4)에서 규정하는 국방정보화사업의 구분에 의하면 국방 AI백신체계는 정보체계 구축 사업의 일환으로 사업분류는 기반운영환경의 사이버 방호체계에 속하며, 획득방법에 의한 분류로는 외주용역 개발에 속하지만 개발사업예산이 국방부에 있지 않은 타부처 R&D사업으로서 적합성 평가 또는 시험평가를 거쳐 실용성 적합 판정을 받은 후에야 상용구매 또는 임차의 형태로 획득하게 되고 운용범위는 전군 지원사업으로 2개군 이상에서 공동으로 운용하는 정보시스템 관련 사업이 된다.

## 2.4 기술개발 실증 개념 및 특징

실증(demonstration)에 대해서는 국내적으로나 해외에서나 다양한 견해가 존재한다. 미 항공우주국에서 과학적·공학적 도전(challenge)과 극복을 위해 필요한 혁신적 기술을 실증임무(TDM, Technology Demonstration Missions)과정을 거치면서 기술 간극을 채우는 사례를 볼 수 있는데 이를 통해 기술적 리스크를 감소시킴과 동시에 NASA 프로젝트와 과업의 비용 효율성을 달성하는 효과를 거두고 있다[2].

한국의 법령에서는 「실증」만을 명확하게 정의하지는 않으나 신기술 인증을 받기 위한 방법 또는 신기술에 대한 사업화를 목적으로 하는 정의가 대부분이며 해외 사례에서도 정부가 개발과정의 기술에 대한 사업화 지원을 주목적으로 하고 있음을 보게 된다[4][5].

[실증과 관련된 국내 관련법·규정]
- 「산업기술혁신 촉진법 시행령」 제18조의2(신기술 인증의 기준 및 대상) 이론으로 정립된 기술을 시작품 등으로 제작하여 시험 또는 운영(이하 "실증화 시험"이라 한다)함으로써 정량적 평가지표를 확보한 개발완료 기술로서 향후 2년 이내에 상용화가 가능한 기술
(산업기술혁신사업 에너지기술 실증연구 평가관리지침) '실증과제'를 '사업화를 목적으로 실제 환경에서 일정기간 이상의 운전을 통해 시제품의 성능을 평가·개선하는 과제'로 정의
- 「기술의 이전 및 사업화 촉진에 관한 법률」,공공·민간영역에서 기술개발 결과의 이전·사업화를 촉진하여 산업 전반의 기술경쟁력 강화와 경제 발전에 이바지하는 것을 목표로 함.
- 「스마트도시 조성 및 산업진흥 등에 관한 법률」,'실증사업' 정의 스마트혁신기술·서비스를 시험·검증하기 위하여 제50조에 따른 승인을 받아 일정기간 동안 규제의 전부 또는 일부를 적용하지 아니하도록 한 사업
- 「환경기술개발사업 운영규정」,'실증화 과제'를 '개발된 기술의 실증설비적용을 위하여 최적화·규모확장 및 주변기술 확보 등을 목적으로 추진되는 과제'로 정의

[해외 실증지원 사례]
- 「미국;주정부와 연계한 실증연구/테스트베드 구축을 통한 사업화지원」 스마트그리드 사업 내 스마트그리드 실증 프로젝트(SGDP, Smart Grid Demonstration Project), 스마트시티 챌린지 등 실증 프로젝트 지원.
- 「일본; 비즈니스 모델(BM) 기반 통합시스템 단위의 실환경 실증 추진」 NEDO(신에너지산업종합개발기구) 주도의 글로벌 협력 프로젝트 및 스마트그리드, 태양광 다용도화 실증 프로젝트, 수소 공급망 구축 실증 등을 추진.
- 「중국; 재생에너지 분야 SoC 보급」 상용화를 위한 시범지구 운영 및 제조업부흥 정책 기반의 실증 지원

연구개발에서 실증 개념을 통해 본 특징을 살펴보면 다음과 같다[5].

• 기술 검증 활동으로 프로토타입, 기술검증을 위한 시험생산 또는 시장에서 받아들여질 것인지를 검증하고 고객 신뢰 확보를 위한 것으로 한정되며

• 공급자 관점 기술검증으로 실험실 단위에서 기술

개발자가 연구개발 산물에 대한 효과성 검증 및 작동 성능의 사전 점검을 목적으로 소규모의 인력과 재원을 투입, 공급자 주도로 기술을 검증하는 시범 사업이다.(테스트베드, 유사환경 검증, 실증 data 등)

• 수요자 관점 시장검증으로, 산업에서 요구되는 Spec, 사용실적, 제도개선, 정부규제 등을 포함하며, 흔히 기술검증 활동과 병행하며 사업화에 근접하도록 기술, 경제, 환경 정보를 제공하고 기술 시제품을 운영함으로써 기술 구현을 수요자 관점에서 평가하는 프로세스이다.(트랙 레코드, 신뢰성, 법·제도 개선 등)

## 3. 연구개발 제품의 실증 프로세스 제안

국방 획득체계나 정보화 분야에서는 시험평가(Test & Evaluation)란 단어에 익숙하고, 실증이란 개념은 가지고 있지 않으며 시행해 본 사례도 없는 실정이다. 여기에서는 현행 국방 관련 규정에서 무기체계나 정보체계 개발 시 시험평가 항목과 절차를 준용하여 민간이나 타 부처 정보보호 신기술의 실증시험 요구사항과 프로세스를 설계하고자 한다.

### 3.1 현행 프로세스 분석

군에서는 기술개발 및 군사 운용 적합도를 평가에서 적용하는 시험평가제도를 두고 있으며 구매, 연구개발, 성능개량 등 획득방법에 따라 특성에 맞는 시험평가 계획 수행결과에 대해 국방전력발전업무훈령 및 합참 무기체계 시험평가 업무규정에서 기술하고 있다. 군에서 시행하는 시험평가의 궁극적 목표는 기술 수준이 완성된 무기체계 또는 전력지원체계에 대해 군 사용 적합 여부를 판단하는 것이다[6][7].

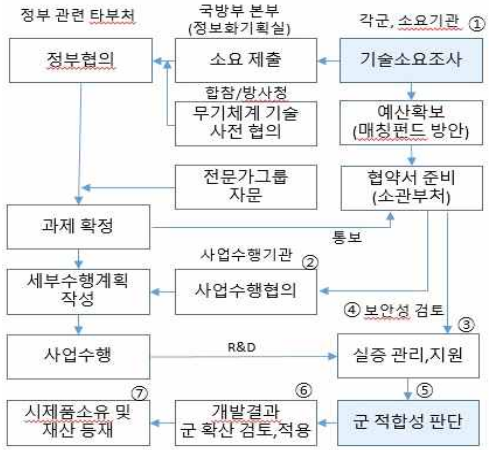
반면, 민간분야에서 개발자들은 개발된 기술에 대한 사업화를 위해서 기술 수준과 성능 수준을 입증하는 과정이 절실하였기 때문에 기업 또는 기술 관련 기관을 중심으로 실증화 시험제도를 정착하게 되었다. 군이 사용할 수 있는 TRL 8·9수준의 기술 이하(보통 TRL 5~8)에서 그 기술 수준과 성능을 입증함으로서 사업화가 가능해지도록 가교역할을 하게 되는 것이다. <표 2>는 군에서 적용하는 시험평가와 실증제도, 타 부처 R&D사업에 대한 적합성 평가의 비교를 나타낸 것이다[7][8].

<표 2> 시험평가 및 실증시험 비교[7][8]

| 구분 | 시험평가(무기체계) | 시험평가(정보체계 구축) |
|---|---|---|
| 개념 | 기술개발 및 군사 운용도 충족도 평가 | 정보화사업의 성공적인 완료 |
| 주체 | 방사청(기품원) 및 합참(소요군) | 소요제기기관 |
| 계획 수립 | 사업통제부서/기관 | 소요제기기관 |
| 시험 환경 | 작전환경, 동등한 조건, 계절별 | 국방정보운용환경(기반운용환경) |
| 평가 수행 | 시험평가단 | 시험평가단 |
| 시험 평가 계획 내용 | 개요, 대상장비/수량, 시평방법, 기간/장소, 시평항목, 기종, 시평단구성, 시평예산, 목표성능, 충족도 평가, 작전가능 여부 | 기술수준(안정성,신뢰성,상호운영성,적용가능성평가 등 목표달성도) 성능수준(운용성, 사업성) 기타 등재논문, 국내/국제표준화 등 |
| 시평 예산 | 사업 예산 내 편성 | 개발부서에서 투입 |
| 평가 방법 | 실물 및 자료, 검증, 확인, 인정(VV&A) | 시연,검사,시험,분석 |
| 판정 | 기준충족/미달, 군사용(전투용) 적합/부적합 | 운용성, 적합성 종합의견 |
| 보안 | 시험평가 계획에 포함 | 보안대책/보안측정 |
| 최종 목표 | 군사용(전투용) 사용 가부 판정 | 기술에 대한 검증,사업화/사회적 가치 실증 |

여기에서 법령 및 규정이 정하는 부분은 평가의 형식과 절차적 양식이며 이 틀이 실효성, 합리성, 수행 용이성을 가지고 역할을 할 수 있도록 오랜 시행을 거치면서 현재에 이르렀다고 할 수 있다.

20년 국방정보화업무훈령을 개정하면서 신기술 및 IT분야의 타부처 개발사업을 신속히 접목할 수 있는 새로운 기술검증에 관한 틀이 마련되었다. 이는 타부처 소관사업에 대한 집행 및 관리규정에 따른 군 적합성 평가에 관한 법령이기는 하지만 실제 이 법령이 적용되어 군에 채택된 개발사업은 찾기 힘들다.




(그림 3) 타부처 소관사업 집행 및 관리[9][10]

또한, 평가의 흐름만 나타나 있고 구체적인 평가항목과 방법에 대해서는 소요제기부서에서 정하여 평가팀이 수행하도록 가이드만 주어져 있을 뿐이다. 따라서 (그림 3)의 ③실증관리 지원 부분에 대한 절차는 미흡하다 할 수 있으며 <표 3>은 훈령에서 언급하고 있는 군 적합성 평가 내용이다[9][10].

<표 3> 타부처 소관 R&D 사업 군적합성 평가[8]

| | |
|---|---|
| 개념 | 군에 적합한 R&D수행이 가능하도록 직간접 참여 |
| 주체 | 국과연, 국방연(외부자문인력) |
| 계획수립 | 소요제기기관 |
| 평가수행 | 평가팀 구성(소요제기기관) |
| 시험평가 계획내용 | 미 정의(구체적 내용은 미 언급) |
| 시평예산 | 미 정의(구체적 내용은 미 언급) |
| 안전및 보안 | 보안대책/보안측정 |
| 최종 목표 | 개발결과에 대한 사업화(구매) 가능 여부 판정 |

## 3.2 국방분야 실증 프로세스 제안

국방 분야에 실증시험에 대한 방법은 무엇을 어떤 목적으로 시험해야 하는가를 올바로 정의하는 것으로부터 시작된다. 앞서 언급한 바와 같이 우리가 실증하려고 하는 국방 AI백신 체계는 기반운영환경의 사이버 방호체계로서 타부처 외주용역 R&D 사업에 속하고, 상용구매 또는 임차의 형태로 획득하게 되는 군내 백신체계에 대한 시험이 될 것이다. 그러면서도 시험의 목적은 타 부처 R&D 사업에 대한 군 적합성 평가에 해당되는 항목을 만족하여야 하는 것이다. 결국 <표 3>을 만족하는 항목과 절차가 명확하지 않기 때문에 시행에 어려움이 있다.

이 과정을 정립하기 위해서 연구개발과제 주관기관이 실증시험 계획에 대한 전반적인 리드를 할 필요가 있고, 한 단계씩 실증기관과 협의하고 컨센서스를 유지하고자 하는 전략적 접근이 필요하다.

## 3.3 국방AI백신에 대한 실증시험 실행 프로세스

먼저, 실증시험을 위한 추진체계는 (그림 4)에서 보는 바와 같이 실증시험 관련 조직(부서)를 파악하고 조직간 업무분장을 조정을 위한 국방부 또는 실증기관과 협의가 필요하다.


(그림 4) 국방 실증시험 실행 단계 절차도[6]

그 다음은 실증 범위, 항목, 절차, 개략 일정 등을 정리한 개략적 실증 추진 계획(안)을 준비하여 협의한다. AI백신 체계가 정보보호체계이므로 보안 적합성 검증을 안보지원사에 요청한다[7]. 실증 환경을 구성하기 위해 국방부 주관으로 실증기관과 대상 네트워크를 선정하고 실증기관 현장 실사를 통해 구체화된 정보를 획득하고 실증시험 계획을 보완하여 보안대책서(안)를 작성하여 국방부를 통해 안보지원사령부에 검토 요청한다. 마지막으로 실증 시험체계 구성을 보완하고 실증시험 기본계획(안)을 마련한다.

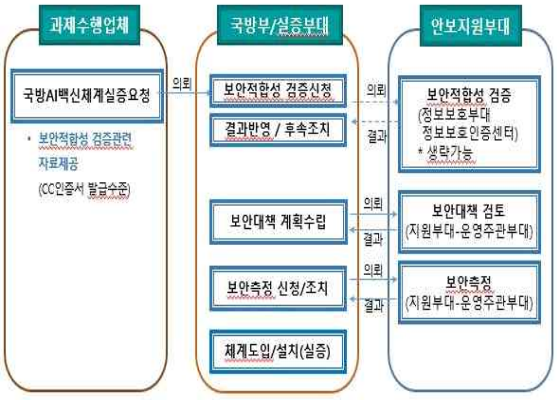
최종적으로 국방부를 통해 합의된 실증계획서를 실증기관에 전파하며, 안보지원사령부에서 보안측정을 받으면 실증 준비가 완료된다. 실증시험은 시험요령에 대한 교육으로 시작하며 군 시험담당자가 참여하여 실증시험이 이루어진다. 시험방법은 합참 무기체계 시험평가 지침에서 정하는 4개 유형의 법을 적용한다. 이때, 실증시험의 내용은 무기체계의 시험평가 수준만큼 완벽성을 지키지는 못하지만 기존 상용 백신 체계가 작동하는 상황에서 미확인된 악성코드를 찾아내는 테스트 기능을 포함, 추가적인 군적합성 평가수준의 실증시험이 되어야 한다. <표 4> 는 시험평가와 실증시험의 비교를 나타내며 주체, 개념, 계획수립, 평가수준 등을 비교한 것이다. 종료 후, 실증시험 결과를 국방부로 보고하며 이 때 관련 기관이 참여하는 협의체를 통해 의견을 종합하고 관련 기관에 통보하면 실증이 종료하게 된다.

<표 4> 시험평가 및 실증시험 비교[8]

| 구분 | 시험평가(무기체계) | 실증시험(정보체계) |
|---|---|---|
| 개념 | 기술개발 및 군사 운용도 충족도 평가 | 창출된 연구성과에 대한 기술성, 안정성을 검증, 사업화로 확산 |
| 주체 | 방사청(기품원) 및 합참(소요군) | 부문별 평가기관 지정 (과기부, 특허청, 시험기관 등) |
| 계획 수립 | 사업통제부서/기관 | 개발사업 총괄부서(기관) |
| 시험 환경 | 작전환경, 동등한 조건, 계절별 | 수요부서 기관의 요구도 |
| 평가 수행 | 시험평가단 | 실증기관 |
| 시험 평가 계획 내용 | 개요, 대상장비/수량, 시평방법, 기간/장소, 시평항목, 기종, 시평단 구성, 시평예산, 목표성능, 충족도 평가, 작전가능 여부 | 기술수준(안정성,신뢰성,상호운영성,적용가능성 평가 등 목표 달성도) 성능수준(운용성, 사업성) 기타 등재논문, 국내/국제표준화 등 |
| 시평 예산 | 사업예산 내 편성 | 개발부서에서 투입 |
| 평가 방법 | 실물 및 자료, 검증, 확인, 인정(VV&A) | 시연,검사,분석 |
| 판정 | 기준충족/미달, 군사용(전투용) 적합/부적합 | 운용성, 적합성 종합의견 |
| 안전 및 보안 | 시험평가 계획에 포함 | 보안대책/보안측정 |
| 최종 목표 | 군사용(전투용) 사용 가부 판정 | 기술에 대한 검증,사업화/사회적 가치 실증 |

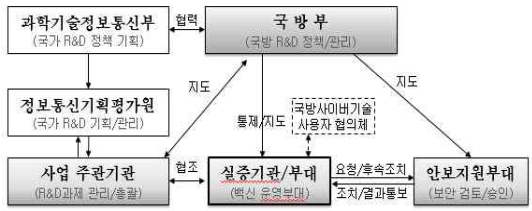
### 3.4 국방분야 실증시 보안성 검토 프로세스

국방부 정보화기획관실 통제 및 감독하에 정보보안 기술개발체계에 대한 실증시험은 진행된다. 실증기관(부대)에서 군사안보지원사령부 예하 지원부대를 통해 국방보안업무훈령 및 국방사이버안보훈령 등에 근거하여 보안적합성검증, 보안대책검토, 보안측정 등 보안업무를 수행하여야 한다.




(그림 5) 국방분야 실증 보안 절차

관련 절차는 (그림 5)와 같이 실증을 위한 신기술 바탕의 보안솔루션 제작 완료 등 준비가 이뤄지고 실증기관(부대)이 선정되는 시기부터 동 시제품의 국방체계 내 적용이 가능토록 보안적합성 검증요청 준비가 되어야 한다. 여기서 한시적 군 시험을 위한 장비는 보안성 적합 대상에서 제외할 수 있다.




(그림 6) 국방분야 실증 보안업무 추진체계[6]

다음은 군 실증 프로세스 상 보안대책의 적절성을 확인하는 절차라고 볼 수 있는 보안대책 검토를 수행하여야 한다. (그림 6)에서 보는 바와 같이 실증기관(부대)에서 국방체계 내에서 실증하는 데 있어 보안 취약점이 없는지와 내부정보 유출, 인원 통제 등의 전반적인 사항을 점검한다[11].

### 3.5 국방분야 실증시험 시범적용 결과 판단

앞서 정의한 실증계획과 실행의 절차에 따라 연구개발 중인 AI백신 체계를 대상으로 국방 분야 실증시험을 제안했던 절차대로 실증시험을 진행하여 실효성을 입증할 수 없으나 전문가 집단에 의해 기존의 시험평가 지침과 비교, 군적합성 여부를 판단할 수 있고 시험평가절차와 마찬가지로 미흡한 사항들을 보완하여 개선할 수 있다.

## 4. 결 론

현존하는 정보보호체계에 추가하여 4차산업혁명의 기술을 시도하는 AI 백신 체계 실증을 국방분야에 적용하여 실증시험하는 것은 군에서나, 개발자 입장에서 의미 있는 일이다. 하지만 군 무기체계에 적용하는 시험평가방법과 같이 엄격한 기준으로 평가하는 방식은 개발자가 사용자가 만족하는 기술개발의 기회를 놓치게 할 수 있다. 적용 과정에서 드러난 불필요한 과정은 협의를 거쳐 실증계획서에서 과감히 제거하고 실용적인 프로세스로 점진적 발전을 시도하여 궁극적으로 민·군이 윈-윈하는 사이버보안 기술 연구개발이 되도록 프로세스 개선이 필요하다.

## 참고문헌

[1] 전정훈, 융합보안논문지, 보안 프로그램의 취약성 및 문제점에 관한 연구, 2012.12.
[2] NASA Space Technology Mission Directorate, https://www.nasa.gov/mission_pages/tdm/main/index.html
[3] 장상수, 융합보안논문지, 정보보호 관리체계 (ISMS)가 기업성과에 미치는 영향에 관한 실증적 연구, 2015.5.
[4] 산업자원부, “산업기술혁신 촉진법 시행령”, 제18조의2(신기술 인증 기준 및 대상), 2019.4.2. 일부 개정.
[5] 김선재, 한국과학기술기획평가원, 연구보고서 정부연구개발 실증사업의 현황 분석, 2018.
[6] 강지원, 융합보안논문지, KOSIGN 기술의 국방 분야 실증시험을 위한 프로세스 개발, 2019.
[7] 국방부, 국방보안업무훈령, 국방부훈령 제2258호, pp.268, 2019.2.13.
[8] 국방부, 국방전력발전업무훈령, 국방부훈령 제2568호 2021.6.30.
[9] 국방부, 전력지원체계 연구개발 업무지침, 2020. 5
[10] 국방부, 국방정보화업무훈령 국방부훈령 제2436호, 2020.6.
[11] 강지원, 융합보안논문지, 미래 지휘통제체계를 위한 보안 규정 개선 요구사항 분석, Vol.20 no.1, pp.69~75, 2020.3.

## 〔저자소개〕

윤 석 준 (Yoon, Sukjoon)

1984년 3월 공군사관학교 항공공학과 학사
1992년 12월 국방대학교 무기체계공학 석사
1998년 7월 독일지휘참모대학 군사학과 석사
현재 세종대학교 연구교수
email : ysjoony@sejong.ac.kr

김 종 현 (Kim, Jonghyun)

1998년 삼성전자 SW연구개발 연구원
2005년 5월 미국 오클라호마주립대 컴퓨터과학과 공학박사
현재 한국전자통신연구원 책임연구원
email: jhk@etri.re.kr

이 상 민 (Lee, Sang-min)

1994년 2월 경북대학교 전자공학과 학사
1996년 2월 경북대학교 전자공학과 석사
현재 한국전자통신연구원 책임연구원
email : sangm@etri.re.kr

강 지 원 (Kang, Jiwon)

1988년 2월 금오공과대학교 전자공학과 학사
1997년 2월 연세대학교 컴퓨터과학과 석사
2012년 8월 경기대학교 정보보호학과 박사
현재 세종대학교 컴퓨터공학과 산학협력중점교수 겸 사이버전연구소 부소장
email : jwkang@sejong.ac.kr