J. Internet Comput. Serv.
ISSN 1598-0170 (Print) / ISSN 2287-1136 (Online)
http://www.jics.or.kr


# 임무 기반의 무기체계 사이버보안 시험평가 적용 연구

# A study on the application of mission-based weapon system cybersecurity test and evaluation

김 익 재[1] 강 지 원[1] 신 동 규[1*]
Ik-jae Kim Ji-won Kang Dong-kyoo Shin

**요 약**

본 논문은 미국 등 선진국에서 적용하고 있는 무기체계 전 수명주기 동안에 사이버보안을 향상 시킬수 있는 방안에 대해 현재까지 진행되고 있는 연구에 대해 알아보고, 국내 무기체계 획득시의 제한사항을 분석하여 효과적인 보안평가 방안을 제시하였다. 국내 실정에 맞는 사이버보안 시험평가 방안에 임무 기반의 위험평가를 획득 전 단계에서 일관성있게 수행함으로써 주요 의사결정 조직에 주요한 정보를 적시에 제공하여 의사결정을 지원하고, 사이버보안 측면에서 식별된 취약점에 대해 보호대책을 검증할 수 있도록 교전규칙을 설정하여 모의침투를 수행하는 방안을 제안하였다. 또한 제안하는 사이버보안 시험평가 체계를 국내 무기체계 시험평가와 비교 평가를 수행하였다. 이를 통하여 지금까지 진행된 사이버보안 시험평가체계 연구에 임무 기반의 위험평가 요소를 접목하여 획득 사업간 적시에 위험을 식별하여 주요 의사결정을 지원하는 역량을 보완하였다.

☞ 주제어 : 사이버보안 시험평가

**ABSTRACT**

This paper examines the ongoing research on ways to improve cybersecurity during the entire life cycle of weapons systems applied in advanced countries such as the United States, analyzes restrictions on obtaining domestic weapons systems, and presents effective security evaluation measures. By consistently performing mission-based risk assessment in the cybersecurity test and evaluation plan suitable for domestic circumstances at all stages of acquisition, important information is provided to major decision-making organizations in a timely manner to support decision-making, and to respond to identified vulnerabilities in cybersecurity. It is proposed to set the rules of engagement so that the protection measures can be verified, and a simulated invasion is proposed. In addition, the proposed cybersecurity test and evaluation system was compared with the domestic weapon system test and evaluation. Through this, the mission-based risk assessment element was grafted into the cybersecurity test and evaluation system research conducted so far to identify risks in a timely manner between acquisition projects, thereby supplementing the capability to support major decision-making.

☞ keyword : cybersecurity test and evaluation

## 1. 서 론

전 세계는 IT(Information Technology) 기술의 급속한 발전으로 사회 전반에 걸쳐 많은 부분에서 소프트웨어의 사용이 증가하고 있다. 가전제품, 자동차, 선박, 항공기 등 모든 분야에서 소프트웨어가 차지하는 비중은 크게 늘어나고 있으며, 이는 국방 무기체계도 마찬가지이다.

국방 무기체계 분야에서 이러한 소프트웨어 비중의 증가는 우수한 성능의 무기체계를 구현하는데 도움을 주기도 하지만 소프트웨어 내부에 잠재적인 취약점이 내재할 수 있으며, 이러한 취약점을 이용한 고도화된 사이버위협에 노출될 가능성 또한 지속적으로 증가하고 있다고 할 수 있다. 특히 우리나라는 사회 전반에 걸쳐 북한에 비해 절대적으로 소프트웨어 활용도가 높기 때문에 이와 같은 비대칭성을 이용해 북한은 노골적으로 사이버 공격을 시도하고 있으며, 이는 전쟁상황에서 아측에 심각한 피해를 발생시킬 수 있는 요소라고 할 수 있다.

이와 같은 사이버 공격에 대응하고자 소프트웨어의 보안 취약점을 제거하기 위한 연구는 지속적으로 이루어지

1 Dept. of Computer Science and Engineering, Sejong Univ., Seoul, 05006, Korea.(209, Neungdong-ro, Gwangjin-gu, Seoul)
* Corresponding author (shindk@sejong.ac.kr)
[Received 6 October 2021, Reviewed 2 November 2021, Accepted 2 November 2021]
☆ 이 논문은 2018년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임 (No.2018R1D1A1B07047395)

고 있으며, 주로 소프트웨어 개발 단계에서 보안 취약점을 유발하는 요소를 사전에 제거하기 위한 소프트웨어 개발보안 연구가 활발하게 진행되고 있다.

이러한 연구 동향은 무기체계에서도 예외가 아니며, 미국은 무기체계 획득단계 전반에 취약점을 효율적으로 식별 및 제거하여 안전하게 전력화하기 위해 사이버보안 시험평가 제도를 적용하고 있으며, 위험관리프레임워크(Risk Management Framework, RMF)라고 하는 사이버보안 제도와 통합하여 운영하고 있다.

이와 관련하여 논문 [1]에서는 미국의 사이버보안 시험평가를 국방 무기체계 획득단계에 적용하는 “무기 획득 사이버보안 시험평가 체계” 도입을 제안하였다. 본 논문은 “무기획득 사이버보안 시험평가 체계”가 기술적·관리적 취약점을 식별한 것에 추가하여 임무 기반의 위험평가를 수행함으로써 사이버 관련 위험을 식별하고 관리가 가능하게 절차를 보완하여 제안한다.

본 논문은 서론에 이어, 2장에서는 관련 연구를, 3장에서는 앞선 [1]에서 제안한 “무기 획득 사이버보안 시험평가 체계”의 제한사항을 살펴보고 4장에서는 임무 기반의 위험평가를 접목하여 사이버보안 평가 제도를 개선하는 방안을 제안한다. 5장에서는 제안하는 사이버보안 시험평가 체계를 국내 무기체계 시험평가와 비교 평가한다.

## 2. 관련 연구

### 2.1 미군의 사이버보안 시험평가 절차와 항목

#### 2.1.1 미군의 사이버보안 시험평가 절차

미국은 사이버보안을 ‘컴퓨터, 전자통신 시스템, 전자통신서비스, 유선통신, 전자통신과 그 안에 담긴 정보에 대해 피해를 방지, 보호, 복원하여 가용성, 무결성, 인증, 기밀성, 부인방지를 보장하는 것을 의미한다’고 정의하고 있다 [2].

시험평가는 무기체계 획득단계의 한 분야로서 시험과 평가의 합성어이다. 시험평가의 주목적은 의사결정에 필요한 정보를 정책결정자에게 적시에 제공하는 것이다 [3]. 시험평가는 무기체계의 객관적인 성능을 검증하고 평가하기 위한 기초 자료를 획득하여 다양한 시험을 통해 사전에 설정된 시험 기준과 비교 분석함으로써 대상 무기체계가 사용자 요구사항에 일치하는지를 검증하고 운용목적에 부합하는지의 적합성을 판단하는 것이다. 이를 통해 무기체계 구매, 연구개발, 설계·제작 등이 소요군의 요구사항에 일치하는가를 판단하는 의사결정 지원단계이다 [1].

미국은 합리적인 사이버보안 시험평가를 위해서 국가차원에서 같은 기준을 적용하고 평가 결과들을 공유할 수 있도록 미국표준기술연구소(National Isntitute of Standard and Technology, NIST)의 사이버보안과 관련된 NIST SP 800 관련 기준문서가 정의되어 있어 시험평가의 합리성과 효율성을 보장한다 [1][4][5][6][7][8][9].

미국 국방부에서는 무기체계의 전 수명주기에 사이버보안을 효과적으로 실현하기 위해 국방 획득 체계에 위험관리프레임워크(RMF)와 사이버보안 시험평가 체계가 통합되어 있으며, 획득 전 단계에 임무 기반의 사이버 위험평가를 적용하고 있다 [1][3][10][11][12].

미국은 무기체계의 전 수명주기 기간 사이버보안을 구현하기 위해 6단계의 사이버보안 시험평가 프로세스를 수행하고 있다. 이러한 프로세스는 무기체계 획득단계 중 최초 소요 분석 단계부터 최종 전력화 단계까지 연속적으로 진행되며 시스템 공학 및 RMF 프로세스 과정과 통합하여 수행된다. 이러한 사이버보안 시험평가 프로세스는 총 6단계로 다음과 같다 [13].

- 1단계, 사이버보안 요구사항 이해: 평가 대상 시스템의 문서를 살펴봄으로써 사이버보안 요구사항을 이해
- 2단계, 사이버 공격표면 식별: 공격자가 시스템을 악용하여 접근 및 침투가 가능한 취약점이 발생할 수 있는 공격표면을 식별
- 3단계, 협업을 통한 취약점 식별: 시험, 분석, 수정, 재시험 과정을 통해 시스템 개발 전반에 걸쳐 사이버보안 취약점을 식별
- 4단계, 적대적 사이버보안 개발시험평가: 3단계에서 작성된 취약점 분석·평가 보고서, 보안평가 보고서 및 개발시험평가 산출물 등을 활용하여 시스템 시험평가 수행
- 5단계, 협업을 통한 취약점 평가 및 침투 평가: 취약점이 발생할 수 있는 임의의 환경에서 시험평가, 이를 통해 대상 시스템에 적용된 사이버보안 수준을 파악
- 6단계, 적대평가: 공인된 취약점 침투 테스트 팀이 이전 사이버보안 시험평가 단계에서 도출된 사이버 위협에 대한 대응방안을 평가

### 2.1.2 미군의 사이버보안 시험평가 항목

미군의 사이버보안 시험평가 항목은 보안통제항목평가팀, 취약점 평가(블루팀), 위협대표 시험(레드팀) 등 평가자원에 따라 표 1과 같이 구분할 수 있다 [13].

(표 1) 평가팀별 시험평가 항목
(Table 1) Test evaluation items by evaluation team

| 보안통제항목 평가팀 | 취약점평가(블루팀) | 위협대표 시험 (레드팀) |
|---|---|---|
| 보안통제항목 준수 평가 | 종합적 취약점 평가 | 하나 이상의 약점 익스플로잇 |
| | 시스템 전체의 알려진 취약점 | 특정 문제나 공격백터 |
| | 보안프로그램의 시스템적 약점 공개 | 시스템 내재된 약점 |
| | | 내외부 위협 |
| | | 정의된 내외부 적의 행동 |

획득 단계별 사이버보안 시험평가 항목은 개발시험평가 단계와 운영시험평가 단계로 구분하여 평가항목을 표 2, 3과 같이 나타낼 수 있다 [13][14][15].

(표 2) 개발시험평가(DT&E) 평가 항목
(Table 2) Development test and evaluation (DT&E) evaluation items

| 기능평가 | 의사결정질문 | 기술 요구사항 |
|---|---|---|
| 시스템 및 소프트웨어 보증 | 시스템과 소프트웨어가 안전하게 개발되었는가? | ·소프트웨어 취약점 제거<br>·보안 소프트웨어 개발 과정(환경)<br>·변조방지 보호 구현<br>·공급망 위험 완화 |
| RMF 요구사항 | 시스템이 사이버보안 기술표준 기준을 만족하는가? | 식별된 공격표면 |
| 취약점 평가 | 노출된 취약점이 시스템 회복력에 악영향을 주는가? | ·시스템 및 네트워크 회복력<br>·사이버킬체인[14] 교란능력<br>·악용탐지, 시스템 저하 복구 |
| 악용된 사이버 취약점에 대응한 시스템 상호운용성 및 기능성 | 시스템이 악용된 사이버 취약점에 대응하여 중요 임무를 지탱할 수 있는 상호운용 가능성과 역량을 갖추었는가? | ·네트워크 관리<br>·정보교환 보장<br>·네트워크 중심의 군사운용 지원<br>·악용된 사이버 취약점에 대한 대응<br>·사이버 경쟁환경에서 군사운용 지원 |

(표 3) 운용시험평가(OT&E) 평가 항목
(Table 3) Operational test and evaluation (OT&E) evaluation items

| 구 분 | 항 목 | 측 정 |
|---|---|---|
| 시스템 보호 데이터 | 취약점 | 사이버 취약점 및 이에 대한 설명 |
| | 침입/권한상승/익스플로잇 | 침입/권한상승/익스플로잇 지점 및 성공/실패, 노력의 수준 등 |
| | 비밀번호 강도 | 크랙을 위해 시도된 비밀번호 수 |
| 시스템 보안 준수 | 계정관리 | 회원가입 등 |
| | 최소 권한 | 최소권한 원칙 |
| | 식별 및 인증 | 고유하게 식별/인증 |
| | 감사기록 내용 | 감사기록의 적절성 |
| | 감사자료 검토, 분석, 보고 | 감사기록의 보고 여부 |
| | 환경설정 | 최소 기능 원칙 준수 |
| | 백업, 복구 및 복원 | 데이터 백업 여부 등 |
| | 기기 식별 및 인증 | 기기의 고유 식별 가능 |
| | 인증자 관리 | 비밀번호, 토큰 등 |
| | 기본 인증자 | 비밀번호, 토큰 등 |
| | 물리적 접근통제 | 데이터 포트 등 |
| | 경계보호 | 방화벽, 가드 IPS 등 |
| | 안전한 네트워크통신 | 통신 및 원격세션 |
| | 관리 업데이트 | 소프트웨어 및 펌웨어 |
| | 악의적인 코드 | 악성코드 방지 등 |
| 사이버보안 성능 데이터 | 보호 | 적대 활동, 공격[15] |
| | 탐지 | 방어자의 공격 탐지 |
| | 대응 | 공격에 대한 완화 |
| | 운용 복원/연속성 | 피해에 대한 복원 |
| | 임무 효과 | 임무 효과의 감소 |

## 2.2 한국의 사이버보안 시험평가 절차와 항목

### 2.2.1 한국군의 사이버보안 시험평가 절차

한국군 무기체계 획득은 '국방전력발전업무훈령' [16]에서 무기체계의 소요, 획득, 운영유지 등 전반전인 수명주기에 대한 지침을 정의하고 있다. 훈령 제52조(무기체계 연구개발)에서는 무기체계 연구개발 절차를 탐색개발단계, 체계개발단계 및 양산단계로 구분하고 있다. 특히 무기체계 도입 단계에서는 사이버보안을 위해 다음과 같은 세부 지침을 제공한다.

- 제52조(무기체계 연구개발) ⑤무기체계 연구개발 시 보안과 관련해 다음 각호의 활동을 수행한다.
  1. 방사청은 탐색개발결과보고서에 무기체계의 정보시스템에 대한 안보지원사의 보호대책 검토결과를 포함하여 제출한다.

2. 방사청은 체계개발 착수 전 안보지원사에 무기체계의 정보시스템에 대한 보호대책 검토를 의뢰하고 검토 결과를 체계개발 계획에 반영한다.
3. 방사청은 체계개발단계에서 내장형SW에 대한 보호대책 검토를 안보지원사에 의뢰하고, 작전운용성능 변경이 요구되거나, 합동성·상호운용성에 영향을 미치는 경우 등 개발계획의 변경이 요구되는 경우에는 국방부(정보화기획관실), 합참, 소요군과 사전 협의하고 안보지원사에 무기체계의 정보시스템 및 내장형SW에 대한 보호대책 검토를 재의뢰해야 한다.

이외에 '국방사이버안보훈령' 제25조, 제26조와 관련하여 안보지원사는 무기체계 탐색개발 및 체계개발 단계에서 무기체계의 정보시스템 및 내장형 SW에 대한 보호대책을 검토하고 무기체계 시험평가 등 전력화 이전 단계에서 보안측정을 수행한다 [16].

### 2.2.2 한국군의 사이버보안 시험평가 항목

한국군의 무기체계 사이버보안 시험평가 항목은 국방전력발전업무훈령 제81조 (시험평가 구분 및 방법)에서 상호운용성 시험평가에 대한 세부사항을 국방상호운용성관리지시를 따르도록 정하였으며, 상호운용성 분야에 정보보증 및 사이버위협 대응과 관련한 시험평가 항목이 포함되어 있다 [16].

전력발전업무훈령에서는 상호운용성 분야에 대한 작성 책임을 합동상호운용성기술센터로 정의하고 있으며, 개발시험평가에서는 소프트웨어 신뢰성 시험과 정보보호를 평가하고 운용시험평가에서는 정보보호만을 평가한다.

국방상호운용성관리지시에 명시된 무기체계에 대한 정보보호 시험평가 항목은 정보보호 수준, 네트워크 정보보호, 관제체계 구축, 키 관리체계 구축, 응용체계, 서버, 단말기, 암호장비 적용, 사이버위협 대응 능력, SW 취약점 제거로 구분되며 세부항목은 표 4와 같다 [17].

## 2.3 무기체계 사이버보안 시험평가 체계

[1]에서 제안한 "무기 획득 사이버보안 시험평가 체계"는 미국에서 적용하고 있는 무기체계 초기부터 체계적으로 사이버보안 시험평가가 진행되는 장점을 국내 사이버보안 프로세스로 제안함으로써 무기체계 획득 및 사이버보안 프로세스와의 연계성을 높여 무기체계 내 사이버보안 적용을 개선하였다. [1]은 국방획득체계 내 사이버보안 단계를 4단계로 구분하고, 각 단계에서 수행해야 할 프로세스를 제안하였다. 특히 개발·운용시험평가 단계에 취약점 분석·평가 및 모의침투를 적용함으로써 적극적으로 취약점을 식별하여 제거하는 프로세스를 추가하였다. 이는 현재 국방분야에서 운영단계에서만 적용하고 있는 취약점 분석·평가와 모의침투를 획득단계에까지 확장하여 사이버보안을 강화한 것이다.

(표 4) 한국군 무기체계 정보보호 시험평가 항목
(Table 4) ROK Military Weapon System Information Security Test Evaluation Items

| 구 분 | 평 가 항 목 |
|---|---|
| 정보보호 수준 | 정보보호 수준의 적절성 |
| 네트워크 정보보호 | 네트워크 정보보호 대책 수립/구현의 적절성 |
| 관제체계 구축 | 관제체계 구축방안 수립/구현의 적절성 |
| 키 관리체계 구축 | 키 관리체계 구축방안 수립/구현의 적절성 |
| 응용체계 정보보호 | 응용체계 정보보호 대책 수립/구현의 적절성 |
| 서버 정보보호 | 서버 정보보호 대책 수립/구현의 적절성 |
| 단말기 정보보호 | 단말기 정보보호 대책 수립/구현의 적절성 |
| 암호장비 적용 | 암호장비 적용계획/적용의 적절성 |
| 사이버위협 대응능력 | 사이버위협 대응능력 |
| | 신분 위장 위협 대응능력 |
| | 데이터 변조 위협 대응능력 |
| | 공격행위 부인 위협 대응능력 |
| | 정보유출 위협 대응능력 |
| | 서비스 거부(DoS) 위협 대응능력 |
| | 권한 상승 위협 대응능력 |
| SW 취약점 제거 | SW 취약점 제거 |
| | 시큐어코딩 규칙 적용 적절성 |
| | 오픈소스 취약점 제거 적절성 |

이러한 [1]의 "무기 획득 사이버보안 시험평가 체계"는 1단계 사이버보안 요구사항 파악, 2단계 사이버 공격표면 식별, 3단계 사이버보안 개발시험평가, 4단계 사이버보안 운영시험평가로 구분되며 세부 내용은 다음과 같다.

- 1단계, 사이버보안 요구사항 파악: 모든 대상 시스템 관련 문서를 살펴봄으로써 사이버보안 요구사항을 파악하고 사이버보안 시험평가 수행을 위한 초기 접근 및 계획 개발
- 2단계, 사이버 공격표면 식별: 공격자가 대상 시스템의 네트워크나 하드웨어, 펌웨어, 물리적 인터페이스, 소프트웨어 등의 접근 가능한 공격 경로를 식별하고 해당 경로에서 발생 가능한 취약점 파악

- 3단계, 사이버보안 개발시험평가: 취약점 분석·평가 보고서, 보안평가 보고서, 개발시험평가 산출물을 활용하여 대상 시스템의 시험평가를 수행
- 4단계, 사이버보안 운용시험평가: 취약점 분석·평가 보고서, 사이버보안 개발시험평가 산출물 등을 참고하여 공격자 입장으로 취약점 침투 테스트를 수행하고 대상 시스템의 사이버보안 정도를 평가

## 3. "무기 획득 사이버보안 시험평가 체계"의 제약사항 : 위험평가 및 위험관리 측면

### 3.1 의사결정 지원을 위한 프로세스 미흡

[1]에서 제안한 "무기 획득 사이버보안 시험평가 체계"는 4단계로 구성되어 있는데 각 단계는 모든 대상 시스템 관련 문서를 살펴봄으로써 사이버보안 요구사항을 파악하고, 대상 시스템의 네트워크, 서버, 펌웨어, 물리적 인터페이스 등을 이용하여 공격표면을 식별한다. 사이버보안 개발 및 운용시험평가 단계에서는 취약점 분석·평가 보고서, 개발시험평가 산출물 등을 활용하여 시험평가를 수행하고 여기에 기술적인 취약점 침투 테스트를 추가해 사이버보안 정도를 평가한다. 이러한 활동의 결과는 기술적·관리적 취약점은 도출할 수 있으나, 사업관리자에게 식별된 취약점으로 인해 발생하는 위험에 대한 정보를 지원하는 것은 고려하지 않았다.

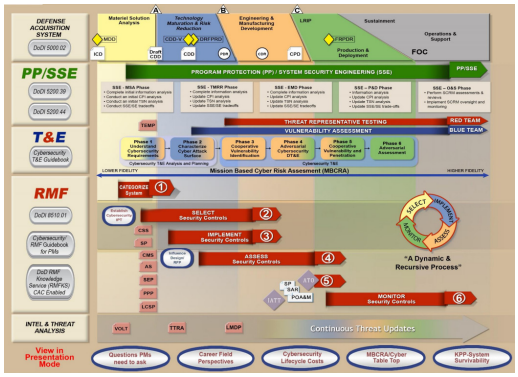
시험평가의 목적은 적시에 의사결정 조직에 주요 의사결정을 위한 정보를 제공하는 것으로 평가결과 식별된 기술적·관리적 취약점을 사업관리자와 소통할 수 있는 수준으로 발전시킬 필요가 있다.

이를 위해 대상 무기체계가 수행하는 임무를 기반으로 사이버에 의존적인 임무를 식별하고 이와 관련된 주요 사이버 위협을 도출함으로써 위험을 식별하고 관리할 수 있는 임무 기반의 위험평가 프로세스의 보완이 요구된다.

CALIT(Cybersecurity & Acquisition Lifecycle Integration Tool)에서는 임무 기반의 사이버 위험평가를 전 획득 수명주기 동안에 지속적으로 수행토록 정의하고 있다 [10].

그림 1은 CALIT에서 임무 기반의 사이버 위험평가를 무기체계 획득 전 기간동안에 수행하는 것으로 묘사하고 있다.

따라서, 본 논문에서는 사이버보안 시험평가를 수행함에 있어 기술적, 관리적 취약점을 식별하여 보완하는 것뿐만아니라 사업관리를 위한 의사결정 조직에 적시에 적절한 정보를 제공하여 의사결정을 지원할 수 있도록 임무 수준의 위험평가를 수행하여 정책결정자와 원활하게 의사소통할 수 있는 프로세스 개선을 제안한다.




(그림 1) CALIT
(Figure 1) CALIT

### 3.2 시험 기준설정 프로세스 미흡

무기체계 획득절차에서 시험평가는 국방전력발전업무훈령에서 운용성확인, 개발시험평가, 운용시험평가로 구분하고 있으며, 특히 작전운용성능 충족 여부 및 군운용적합 여부를 판단하는 운용시험평가는 사전에 시험 기준이 명확히 설정되어 시험평가기본계획서(TEMP)에 반영되어야 한다. 이러한 측면에서 [1]에서 제안한 "무기획득 사이버보안 시험평가 체계"는 취약점 분석·평가와 모의침투 기술을 접목하여 획득단계에서 취약점을 식별하기 위한 프로세스를 보완하였으나, 도입하는 무기체계의 취약점을 모두 완벽하게 제거하는 것은 현실적으로 제한되며 획득기간이 장기화 될수록 새로운 위협은 추가 발생할 수 있어 모든 취약점을 완벽하게 제거하는 것을 시험평가의 기준으로 삼기에는 부적절하다. 따라서 식별된 취약점을 완화하기 위한 적절한 보호대책을 도출하여 이를 시험평가 단계에서 검증하는 것을 시험평가의 기준으로 삼아 전투용 적합을 판정하는 것이 합리적이라고 할수 있다.

물론 식별된 취약점에 대한 보호대책이 실효성이 없는 경우에는 시험평가에서 전투용 부적합을 판단하여 재시험토록 강제할 필요가 있다. 이는 사업 예산과 기간 등 자원이 한정된 무기체계 획득단계에서 효과적으로 취약점을 제거하고, 관리하기 위한 대안이 될 것이다. 이러한 과정은 취약점을 완화하기 위한 정보를 제공하여 예산을

효율적으로 사용토록 의사결정을 지원할 수 있다.

식별된 취약점을 완화하는 효율적인 방안으로는 [14]의 사이버 킬체인 개념을 적용하면 더욱 효과적인 보호대책을 도출할 수 있을 것이다.

본 논문에서는 취약점 완화를 위한 보호대책의 실행 우선순위는 고려하지 않았으며, 시험평가 기준설정을 위한 프로세스를 보완하여 식별된 취약점에 대한 보호대책의 실효성을 검증하기 위해 모의침투에 대한 교전규칙 설정을 제시한다.

## 4. 제안하는 임무 기반의 사이버보안 시험평가

이 장에서는 한국군에 적합하도록 [1]에서 제안한 “무기 획득 사이버보안 시험평가 체계”에 임무 기반의 위험평가를 연계한 개선된 사이버보안 시험평가를 제안하고자 한다. 제안하는 임무 기반의 사이버보안 시험평가는 [1]에서 제안한 “무기 획득 시이버보안 시험평가 체계” 4단계에 따라 다음 표 5와 같이 수행한다.

(표 5) 사이버보안 시험평가 단계 구분
(Table 5) Classification of cybersecurity test and evaluation stages

| 구분 | [1] | 제안 |
|---|---|---|
| 1단계 | 사이버보안 요구사항 이해 | 위협/위협 모델링 |
| 2단계 | 사이버 공격표면 식별 | 공격표면 목록화 |
| 3단계 | 사이버보안 개발시험평가 | 공격표면 취약점 분석·평가 |
| 4단계 | 사이버보안 운용시험평가 | 교전규칙 기반의 모의침투 및 취약점 분석·평가 |

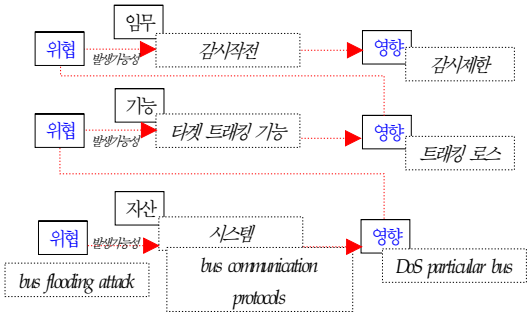
이는 1~2단계에서 위험과 위협에 대해 모델링을 하고, 공격표면을 식별하여 목록화를 수행한다. 3단계에서는 공격표면에 대한 취약점 분석·평가를 바탕으로 임무 기반의 위험평가를 수행하여 취약 자산에 대해 보호대책을 도출한다. 4단계에서는 보호대책의 실효성을 검증하기 위한 교전규칙을 설정한 가운데 모의침투 및 취약점 분석·평가를 재수행한다. 이때 보호대책이 모의침투에 의해 무력화될 경우 보호대책을 보완하고 재시험을 수행한다. 보호대책의 실효성이 검증된 이후에 임무 기반의 위험평가를 수행하여 위험도가 요구수준을 충족한 경우에 전투용 적합을 판정하고 무기체계를 전력화한다.

각 단계별 세부내용은 다음과 같다.

### 4.1 위험/위협 모델링

1단계, 위험/위협 모델링은 [1]의 사이버보안 요구사항 파악 단계에서 수행하며, 임무 기반의 위험평가를 위해 전력소요서 기반의 초기 위험/위협 모델링을 수행한다.

임무 기반의 위험평가를 위해 사이버 의존적인 임무를 식별하고, 임무에 대한 세부 기능을 세분화하며 그림 2와 같이 도식한다.

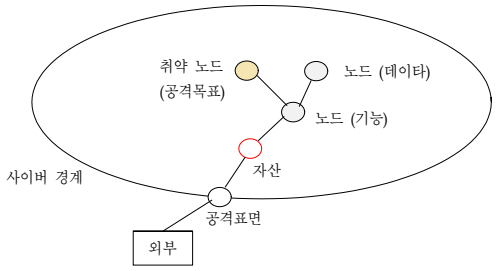



(그림 2) 위험/위협 모델링(예)
(Figure 2) Risk/threat modeling (example)

### 4.2 공격표면 목록화

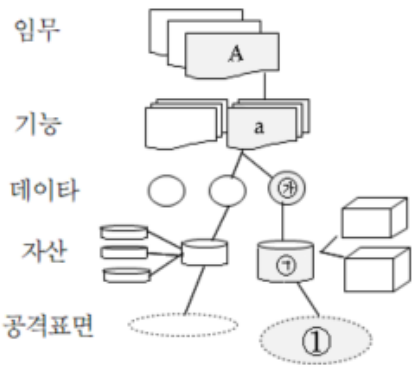
2단계, 공격표면 목록화는 [1]의 사이버 공격표면 식별 단계에서 수행하며, RFP 등 보완된 문서를 기반으로 위험/위협 모델링을 재차 수행하고 공격표면을 목록화한다.

공격표면의 식별은 무기체계를 중심으로 사이버 경계를 설정하고 이를 통해 외부에서 시스템으로 접근하는 진입점을 공격표면으로 식별하며 시스템으로 진입하는 자산부터 시스템의 노드들을 단계별로 구분하여 표현한다. 이때 취약점이 있는 노드는 공격목표가 되는 주요한 노드가 된다. 이를 그림으로 표현하면 그림 3과 같다.




(그림 3) 무기체계의 공격표면 식별
(Figure 3) Identification of the attack surface of a weapon system

식별된 공격표면은 무기체계의 임무부터 하위 기능, 데이터, 자산을 식별하여 그림 4와 같이 도식화 할 수 있다. 이렇게 하면 공격표면이 어느 자산을 통해 어떠한 데이터를 처리하고 무슨 기능을 수행하는지와 최종적으로 달성하고자 하는 임무를 연결지을 수 있다.




(그림 4) 사이버 의존적인 임무의 공격표면 식별
(Figure 4) Identify the attack surface of cyber-dependent missions

공격표면 식별 단계를 통해 임무 기반의 위험평가를 위한 필요 요소는 도출하였으며, 이를 통해 시스템 수준의 위협 시나리오를 작성하면 "공격자는 공격표면 ①을 통해 자산 ㉠의 취약점을 이용하여 데이터 ㉮를 탈취 또는 변조한다."고 할수 있다. 이를 사업관리자의 관점에서 의사결정을 지원하기 위해서는 임무 수준으로 발전시킬 필요가 있으며 그 예시는 "공격자는 공격표면 ①을 통해 자산 ㉠의 취약점을 이용하여 데이터 ㉮를 탈취 또는 변조하여 a기능의 신뢰성이 저하되었고, 임무 A의 수행이 제한된다."라고 표현할 수 있다. 표 6은 시스템 수준의 위협 시나리오와 임무 수준의 위협 시나리오의 발전 관계를 보여준다.

(표 6) 수준별 위협 시나리오
(Table 6) Threat Scenarios by Level

| 구 분 | 위협 시나리오 |
|---|---|
| 시스템 수준 | 위협원 → 위협 행위 → 취약점(이용) → 영향성 판단(자산) |
| 임무 수준 | 위협원 → 위협 행위 → 취약점(이용) → 영향성 판단(자산, 기능, 임무) |

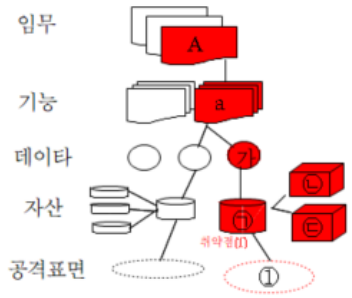
## 4.3 공격표면 취약점 분석·평가

3단계, 공격표면 취약점 분석·평가는 개발시험평가 단계에서 수행하며, 개발문서 기반으로 위협/위협 모델링을 재차 수행하고 공격표면에 대한 취약점 분석·평가를 수행한다.

공격표면에 대한 취약점 분석·평가를 수행하면 자산 레이어에서 취약한 자산이 식별되고, 이와 연계된 데이터와 기능이 식별된다. 이를 바탕으로 취약한 임무를 식별할 수 있다.

그림 5는 공격표면에 대한 취약점 분석·평가를 통해 취약한 공격표면으로부터 취약 자산 및 취약 데이터, 사이버 의존적인 기능과 임무를 식별한 모습이다.

이를 이용해 위협 시나리오를 보완하면 "자산 ㉠은 취약점 (1)이 식별되었으며 이를 이용해 자산 ㉡과 ㉢이 장악되고, 이와 관련된 데이터 ㉮가 탈취 또는 변조될 수 있다. 이로인해 기능 a가 제한되어 결과적으로 임무 A를 수행할 수 없다"고 설명할 수 있다.

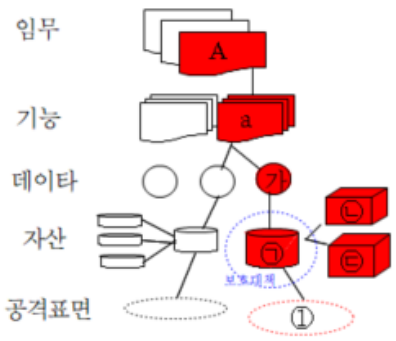



(그림 5) 공격표면 취약점 분석·평가에 따른 취약점 식별
(Figure 5) Identification of vulnerabilities according to attack surface vulnerability analysis and evaluation

이에 따라 사업관리자는 취약점에 대한 보호대책을 강구하여 위험을 완화토록 조치할 수 있다.

그림 6은 취약한 자산 ㉠에 대하여 취약점(1)을 완화하기 위한 보호대책을 도출하고, 도출된 보호대책을 청색 점선으로 자산 ㉠의 테두리에 표시하였다.

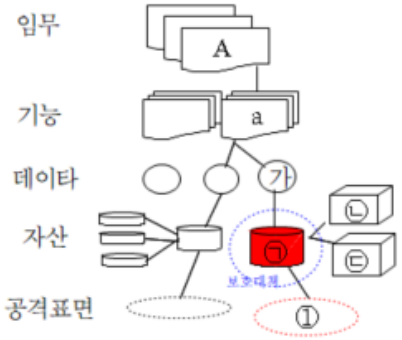
이렇게 보호대책으로 보완된 취약점은 전체 무기체계의 위험을 완화할 수 있으며, 자산 ㉠에 대해 보호대책을 강구함으로써 그림 7에서 처럼 자산 ㉡과 ㉢은 정상 상태로 환원되었다. 그 결과로 데이터 ㉮와 기능 a, 임무 A는 모두 정상 상태를 나타내고 있다. 이러한 조치를 바탕으




(그림 6) 취약 자산에 대한 보호대책 도출
(Figure 6) Deriving protection measures for vulnerable assets

로 임무 기반의 위험평가를 수행할 수 있으며, 그 결과는 의사결정 조직에 보고되고 빠른 시간에 의사결정할 수 있도록 제공됨으로써 무기획득 과정의 소통을 원활하게 만든다.

특히 무기체계 획득 기간이 장기간 소요되는 경우 한정적인 사업기간과 사업예산 범위 내에서 고속으로 발전하는 위협을 모두 완벽하게 제거하는 것은 현실적으로 제한된다. 따라서 이러한 과정을 통해 위험을 관리할 필요가 있다.




(그림 7) 보호대책을 통한 취약점 완화
(Figure 7) Mitigation of vulnerabilities through protection measures

이렇게 공격표면별로 발생 가능한 모든 위협 시나리오는 모의침투를 위한 교전규칙으로 설정할 수 있으며, 각 자산에 대한 보호대책의 실효성을 검증할 수 있는 기준이 된다.

### 4.4 교전규칙 기반의 모의침투 및 취약점 분석·평가

4단계, 교전규칙 기반의 모의침투 및 취약점 분석·평가는 운용시험평가 단계에서 수행하며, 앞서 식별된 공격표면별 위협 시나리오를 교전규칙으로 하여 모의침투를 수행한다.

위협 시나리오는 공격표면 ①을 통하여 청색 점선의 보호대책을 무력화하는 것이며, 자산 ㉠의 취약점 (1)을 이용해 임무 A를 수행하지 못하도록 모의침투를 수행하는 것이다.

이를 통해 최초 식별된 공격표면의 취약점을 이용해 위협 시나리오를 따라 모의침투를 수행하여 강구된 보안대책의 실효성을 검증한다. 교전규칙 기반의 모의침투를 통해 자산 및 데이터, 기능, 임무의 위험 완화 상태를 검증하고 그 결과를 토대로 임무 기반의 위험평가를 수행한다. 이때 취약점이 지속적으로 확인될 경우에는 보안대책을 보완한후 재시험을 통해 재검증하여 전력화 이전에 안전한 상태를 보장한다.

이로써 공격표면 식별 단계에 작성된 임무 기반의 위협 시나리오를 토대로 위험평가, 취약점 분석·평가, 보호대책 강구, 교전규칙 설정, 모의침투 수행 등의 사이버보안 시험평가 활동이 진행된다.

## 5. “무기 획득 사이버보안 시험평가 체계”와 제안 방안 비교평가

[1]의 “무기 획득 사이버보안 시험평가 체계”는 사이버보안 관점에서 국내 무기체계 시험평가에 미국의 사이버보안 프로세스를 접목하여 사이버보안을 강화하도록 제안한 방안이다.

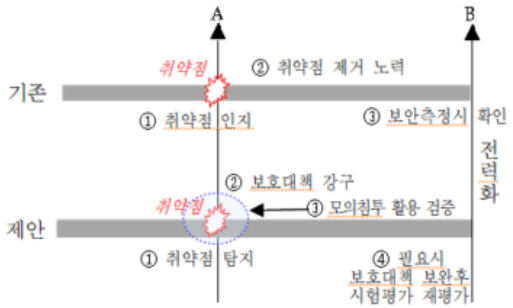
본 논문에서는 이러한 [1]의 “무기 획득 사이버보안 시험평가 체계”에 임무 기반의 위험평가를 추가하여 단계별로 반복적인 위험/위협 모델링을 수행하고, 임무 기반의 위협 시나리오를 바탕으로 취약점 분석·평가와 교전규칙 설정하 모의침투를 실행함으로써 운용시험평가 단계에서 보안대책의 실효성을 검증할 수 있는 체계를 개선하여 제안하였다. 또한 시험평가 수행을 위한 가이드라인으로 교전규칙을 설정하고 대응이 미흡한 경우에는 재시험을 통해 무기체계의 보호대책을 보완토록 하여 보다 강화된 사이버보안 구현을 강조하였다.

사이버보안 관점으로 국내 무기체계 시험평가와 제안 방안을 비교하면 표 7과 같다.

(표 7) 국내 무기체계시험평가와 비교
(Table 7) Comparison with domestic weapon system test and evaluation

| 구 분 | 국내시험평가 | [1] | 제 안 |
|---|---|---|---|
| 위협 시나리오 | 없음 | - | ○ |
| 위험평가 | 없음 | - | ○ |
| 취약점 분석·평가 | 1회 | 3회 | 3회 |
| 모의침투 | 없음 | 1회 | 1회 |

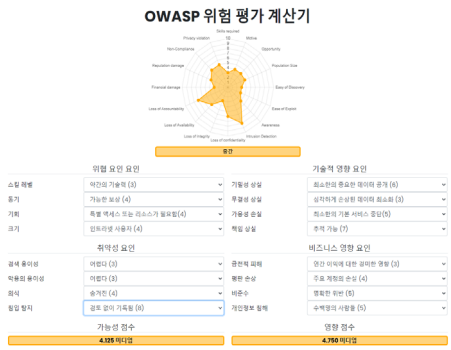
또한, 제안한 방안은 국방 무기체계 획득 과정에서 취약점을 식별하는 A지점부터 전력화하는 B지점 까지 취약점에 대응하는 관점에서 개선되는 사항은 그림 8과 같다. 이는 취약점을 능동적으로 탐지하여 보호대책을 강구하고, 기술적 검증과정을 거쳐 시험평가 요소에 반영함으로써 부적합시 재평가하는 적극적인 통제 효과가 있다.



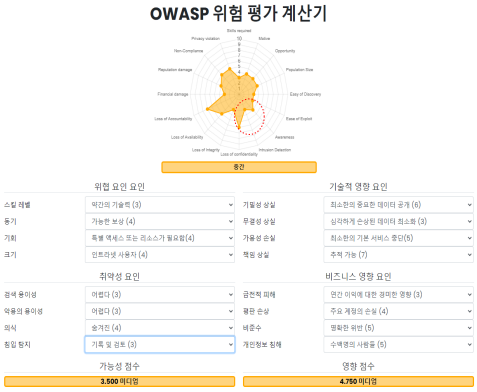

(그림 8) 제안한 방안 적용시 개선 사항
(Figure 8) Improvements when applying the proposed method

OWASP 위험평가 계산식은 위협, 기술적 영향성, 취약성, 비즈니스 영향성의 4개 분야별로 위협은 스킬, 동기, 기회, 사용자로 기술적 영향성은 기밀성, 무결성, 가용성, 책임으로 취약성은 검색 용이성, 악용 용이성, 의식, 침입탐지로 비즈니스 영향성은 금전, 평판, 비준수, 개인정보 등의 백터를 이용해 위험평가를 계산하고 있다 [18].

본 논문에서 제안한 임무 기반의 사이버보안 시험평가 체계는 OWASP 위험평가 계산식에 의해 침입탐지 지수를 향상시킬 수 있다. 그림 9와 그림 10은 가상의 위험평가에서 논문에서 제안한 프로세스를 통해 침입탐지 지수가 향상된 경우 전체 위험평가 결과가 향상되는 결과를 보여주고 있다. OWASP 위험평가 계산식에서는 취약점을 사전에 검토하지 못한 경우를 위험지수 8로 설정하고 있으며, 취약점을 검토하고 기록하는 경우는 위험지수를 3으로 설정하고 있다.




(그림 9) 침입탐지가 검토없이 기록된 경우의 위험평가 계산
(Figure 9) Calculation of risk assessment when intrusion detection is recorded without review




(그림 10) 침입탐지가 검토되고 기록된 경우의 위험평가 계산
(Figure 10) Risk assessment system where intrusion detection is reviewed and recorded

따라서 본 논문에서 제안한 임무 기반의 사이버보안 시험평가 절차를 수행하면 침입탐지 지수를 향상시켜 전체적인 위험을 완화할 수 있는 효과가 있다고 할 수 있다.

## 6. 결 론

본 논문에서는 미국의 사이버보안 시험평가를 토대로 앞서 연구된 국내 실정에 맞는 사이버보안 시험평가 방

안에 임무 기반의 위험평가를 획득 전 단계에서 일관성 있게 수행함으로써 주요 의사결정 조직에 주요한 정보를 적시에 제공하여 의사결정을 지원하고, 사이버보안 측면에서 식별된 취약점에 대해 보호대책을 검증할 수 있도록 교전규칙을 설정하여 모의침투를 수행하는 방안을 제안하였다.

이는 획득단계 전반에서 관련 조직간의 의사소통을 원활하게 할 수 있으며, 정보공유를 통해 취약점을 보완하고 그 실효성을 검증하며 미흡한 경우에는 재시험할 수 있도록 제도화하여 획득하는 무기체계의 사이버보안 능력을 향상시킬 것으로 판단된다.

그러나 본 논문의 제한사항은 장기간 소요되는 무기체계 획득기간에 사업관리자와 무기체계 소요군 및 사이버보안 책임자의 원활한 의사소통을 위한 방법은 지속 발전시킬 필요가 있다. 그런 측면에서 미국에서 사용하고 있는 CTT(Cyber Table Top) 방식의 단순화된 구술 워게임 방식은 비용적인 측면에서 효과적인 의사소통 수단이 될 수 있을 것으로 판단된다. 향후 추가되는 연구에서는 CTT를 접목하여 의사소통하는 방안과 위험평가를 위한 세부 방법론의 구체화가 요구된다.

또한 식별된 취약점에 대한 보호대책 수립 우선순위에 대한 연구도 구체화가 필요하며, 최적의 보호대책을 대상으로 모의침투에 대한 교전규칙 설정이 필요하다고 할 수 있다.

그럼에도 불구하고 본 논문은 미국 및 선진국에서 추구하는 무기체계 전 수명주기 동안에 사이버보안 활동을 강화하고 위험을 관리하기 위한 노력이 지속되고 있음을 고려할 때 국내 무기체계에 적용할 수 있는 사이버보안 시험평가를 위한 하나의 방법론 구체화에 기여하였다고 할 수 있다.

## 참고문헌(Reference)


[1] Ji-seop Lee, Sung-yong Cha, Seung-soo Baek, Seung-joo Kim, " Research for Construction Cybersecurity Test and Evaluation of Weapon System", Journal of The Korea Institute of information Security & Cryptology Vol.28, No.3, Jun. 2018. https://doi.org/10.13089/JKIISC.2018.28.3.765

[2] THE WHITE HOUSE WASHINGTON, "National Security Presidential Directive-54/Homeland Security Presidential Directive-23", January 8. 2008.

[3] Jong Wan Park, "The Action of the Reliability Enhancement in Test and Evaluation of the Weapon Systems", Journal of Applied Reliability Vol. 15-2, pp. 108-123, 2015.

[4] Congressional Research Sercive, Defense Acquisitions: How DOD Acquires Weapon Systems and Recent Efforts to Reform the Process. May 23, 2014.

[5] "Guide for Conducting Risk Assessment", NIST SP 800-30 Rev.1. 2012.

[6] "Guide for Applying the Risk Management Framework to Federal Information systems", NIST SP 800-37 Rev.1. 2010.

[7] "Managing Information Security Risk", NIST SP 800-39, 2011.

[8] "Security & Privacy Controls for Federal Information Systems and Organizations", NIST SP 800-53 Rev.4, 2013.

[9] "Guide for Assessing the Security Controls in Federal Information Systems and Organizations", NIST SP 800-53A Rev.1, 2010.

[10] "Cybersecurity & Acquisition Lifecycle Integration Tool(CALIT)", DAU ver 3.1, sep 2018.

[11] Hyun-suk Cho, Sung-yong Cha, Seung-joo Kim, "A Case Study on the Applicaion of RMF to Domestic Weapon System", Journal of The Korea Institute of Information Security & Cryptology Vol.29, No.6, Dec.2019.

[12] Sungyong Cha, Seungss Baek, Sooyoung Kang and Seungjoo Kim, "Security Evaluation Framework for Military IoT Devices", Security and Communication Networks. Vol. 2018, Article ID 6135845, 12 pages, Jul. 2018.

[13] Department of Defense, "Cybersecurity Test and Evaluation Guidebook", 2015.

[14] Jung-Sik Lee, Sung-Young Cho, Heang-Rok Oh, Myung-Mook Han, "A Study on Defense and Attack Model for Cyber Command Control System based Cyber Kill Chain", Journal of Internet Computing and Services Vol. 22, No. 1, pp. 41-50, Feb. 2021. https://doi.org/10.7472/jksii.2021.22.1.41

[15] Uihyeon Song, Donghwa Kim, Myung Kil Ahn, "Layered Authoring of Cyber Warfare Training Scenario", Journal of Internet Computing and Services,

Vol. 21, No. 1, pp. 191-199, Feb. 2020.
https://doi.org/10.7472/jksii.2020.21.1.191
[16] “National Defense Power Generation Business Instruction”, Ordinance of the Ministry of National Defense, 2021.
[17] “Defense Interoperability Management Directive”, Ministry of National Defense, Jan. 2021.
[18] https://javaierolmedo.github.io/OWASP-Calculator, 2021.

## ◐ 저 자 소 개 ◑

**김 익 재(Ik-jae Kim)**
1995년 공군사관학교 전산과학과(이학사)
2007년 국방대학원 전산정보학과(공학석사)
관심분야 : 정보보호, 사이버보안 T&E, RMF, etc.
E-mail : nodo2@naver.com

**강 지 원(Ji-won Kang)**
1988년 금오공대 전자공학 학사
1997년 연세대학교 컴퓨터과학 (정보보호 전공) 석사
2012년 경기대학교 정보보호학 박사
2017년~현재 세종대학교 컴퓨터공학과 산학협력중점교수
E-mail : jwkang@sejong.ac.kr

**신 동 규(Dong-Kyoo Shin)**
1986년 서울대학교 컴퓨터과학과(공학사)
1992년 Illinois Institute of Technology 대학원 컴퓨터공학과(공학석사)
1997년 Texas A&M University 대학원 컴퓨터과학과(공학박사)
1998년~현재 세종대학교 컴퓨터공학과 교수
관심분야 : 머신러닝, 유비쿼터스 컴퓨팅, 생체신호 데이터처리, 정보보호, etc.
E-mail : shindk@sejong.ac.kr