논문접수 2021.08.22 | ISSN 1738-6144 | Journal of The Korea Association of Defense Industry Studies Vol. 28, No. 2(2021)
논문확정 2021.09.10 | http://journal.kadis.or.kr/ | 한국방위산업학회지 제28권 제2호 | http://doi.org/10.52798/KADIS.2021.28.2.4

무기체계 안티탬퍼링을 위한 기술 식별 및 위험평가 방안

Technology Identification and Risk Assessment for Anti-Tampering of Weapon Systems

송경호**, 허아라***, 류연승****
Kyungho Song**, Ara Hur***, Yeonseung Ryu****

ABSTRACT

The Korean defense industry is taking a leap forward into the global market by securing international competitiveness. Recently, threats targeting defense science and technology are increasing, researchers are moving abroad illegally, and cyber hacking attacks are occurring, so the need for anti-tampering is also required to protect the technology of weapon systems for export. Anti-tampering is the engineering protection measure to delay and prevent technology leakage through reverse engineering of weapon systems. The United States, a major arms export country, has long applied anti-tampering to protect the technology of weapon systems. Though Korea enacted the Defense Industry Technology Protection Act and focused on activities to prevent technology leaks from defense industry, no technical protection activities are being carried out for weapons systems, and there is no guideline for technology protection of weapon systems. In this paper, we propose a method for identifying defense technology to be protected in the anti-tampering process and a risk assessment method for determining whether to apply anti-tampering. The proposed method can be used to develop anti-tampering guideline to be applied to weapon system acquisition and R&D procedure by the Defense Acquisition Program Administration and R&D institutions.

초 록

우리나라 방위산업은 국제경쟁력 확보 및 세계시장 진출 단계로 도약하고 있다. 최근 국방과학기술을 노리는 위협이 증가하고 있고 연구원의 불법 국외 이직, 사이버 해킹 공격이 발생하고 있어 수출용 무기체계의 기술보호를 위한 안티탬퍼링 필요성도 요구되고 있다. 안티탬퍼링은 무기체계의 역설계를 통한 기술 유출을 지연, 방지하기 위한 공학적 보호조치이다. 주요 무기수출국인 미국은 오래전부터 무기체계의 기술보호를 위해 안티탬퍼링을 적용하고 있다. 우리나라는 방위산업기술보호법을 제정하고 방산업체의 기술 유출을 방지하기 위한 활동에 중점을 두고 있으나 아직까지 무기체계의 기술보호를 위한 활동은 미미하고 관련 지침도 부재한 실정이다. 본 논문에서는 무기체계의 안티탬퍼링 적용을 위해 보호할 방산기술의 식별과 안티탬퍼링 적용 여부를 결정하는 위험평가 방안을 제안하였다. 제안한 방안은 방위사업청 및 연구개발기관이 무기체계 획득과 연구개발 절차에서 사용할 안티탬퍼링 지침의 개발에 활용할 수 있다.

Key Words : Anti-Tampering(안티탬퍼링), Weapon System(무기체계), Technology Protection(기술보호), Technology Identification(기술 식별), Risk Assessment(위험평가).

* 본 연구는 방위사업청과 국방과학연구소(계약번호: UD200026ED)의 지원에 의한 연구 결과임.
** 송경호, 명지대학교 보안경영공학과 박사과정
*** 허아라, 명지대학교 보안경영공학과 박사수료
**** 류연승, 명지대학교 보안경영공학과 교수(교신저자 E-mail: ysryu@mju.ac.kr)

Ⅰ. 서 론

방위사업청은 2015년 방위산업기술보호법을 제정하고 방위산업과 관련한 국방과학기술 중 국가안보 등을 위하여 보호되어야 하는 기술을 방위산업기술(이하 방산기술이라 부름)로서 지정·고시하고 있다[1]. 국방과학기술의 수준이 세계 8위로 평가되고 첨단 무기체계의 독자개발과 수출이 증가하면서 국외에서 우리 방산기술을 탈취하려는 시도가 증가하고 있다. 대표적으로 2020년 ADD 연구원의 국외 불법취업, 2021년 한국항공우주산업의 사이버 해킹 공격 등이 있다.

국방 선진국은 자국 방산업체의 연구원, 기술자료의 보호를 위해 인원, 시설, 정보 등의 보호체계를 제도적으로 구축하고, 나아가 무기체계의 역설계를 통한 기술 유출 방지를 위해 안티탬퍼링(Anti-tampering) 제도를 운용하고 있다. 안티탬퍼링은 무기체계의 기술을 보호하기 위한 공학적 활동으로서, 중요기술에 대한 비인가자의 접근을 차단 또는 지연시켜 기술 유출에 대비하는 것이다[2-6]. 무기체계 수입국에서 역설계 등을 통해 무기체계의 기술을 유출하거나 무단 변경하여 무기체계 복제 또는 대응수단 개발에 사용한다면 그 무기를 개발한 국가는 투입된 노력과 시간이 무의미하게 되고 동시에 국가경제와 국가안보에 대한 위협으로도 작용한다.

우리나라 방위산업은 수출 진흥 정책과 함께 무기체계의 국외수출이 증가함에 따라, 방위사업청은 수출용 무기체계에 안티탬퍼링 적용을 의무화할 예정이다. 그러나, 방위사업청 및 연구개발기관이 무기체계 획득과 연구개발 절차에 적용할 안티탬퍼링 지침이 아직 없으며 이에 대한 연구도 미미한 실정이다.

국내 무기체계 안티탬퍼링 프로세스 관련 선행연구는 거의 없으며, [3, 4]에서 제안한 안티탬퍼링을 적용한 수명주기 프로세스 모델이 유일하다. 제안한 프로세스에서 기술 식별은 연구개발 단계 종료시점에서 기술성숙도 평가를 통해 식별하고 있다. 또한, 기술이 구현된 구성품에 대한 위험평가를 하지만 위협 분석은 다루고 있지 않다.

본 연구에서는 국방 선진국인 미국의 안티탬퍼링 제도의 분석을 통해 국내 안티탬퍼링을 위한 기술 식별과 위험평가 방안을 제안하였다. 제안한 방안은 선행연구와는 다르게 무기체계 획득 수명주기의 시작 단계부터 기술 식별을 반복하여 구성품 수준까지 식별한다. 또한, 구성품에 대해 위협 분석을 포함한 위험평가를 수행하여 효과적인 안티탬퍼링 기법을 결정할 수 있게 해준다.

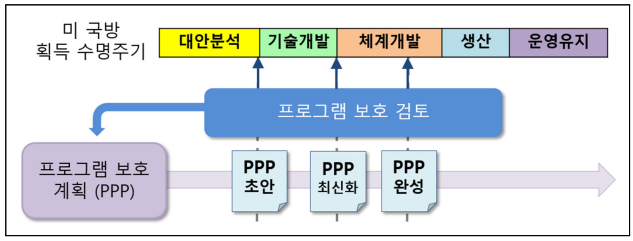
본 논문의 구성은 다음과 같다. 2장에서 미국의 프로그램 보호 제도 및 안티탬퍼링 제도를 간단하게 소개한다. 3장에서 우리나라 안티탬퍼링 프로세스에서 사용할 기술 식별 및 위험평가 방안을 제안하고 4장에서 논문의 결론 및 정책 제언을 기술한다.

Ⅱ. 미 국방부 관련 제도

2.1. 프로그램 보호 계획

미국 국방부는 무기체계 획득 프로그램의 보호를 위해 프로그램 보호 계획(Program Protection Plan: PPP)[1]을 수립하고, 무기체계 수명주기 전반에 걸쳐 관리하고 있다[7-16]. 무기체계 안티탬퍼링은 프로그램 보호 계획의 일부로서 검토되고 안티탬퍼링 적용이 결정되면 안티탬퍼 계획(AT Plan)을 수립하고 PPP 문서에 첨부한다.

PPP 수립은 획득 수명주기의 초기 단계부터 시작하며 〈그림 1〉에서 보듯이 기술검토회의 단계마다 PPP를 최신화하여 검토하고 완성해나간다.



〈그림 1〉 획득 수명주기 간 PPP 수립 [16]

프로그램 보호 계획에서 보호 대상은 〈표 1〉에서 보이듯이 크게 3개로서, ① 기술(technology), ② 구성품(component), ③ 획득 프로그램의 정보(informaton)이다. 프로그램 보호는 이 3개 보호 대상에 대하여 위협(threat), 취약성(vulnerability) 및 공격(attack)을 평가하고, 공격에

주1) PPP는 무기체계 및 지원체계에 대한 안정성과 보안성을 확보하고 각종 위협에 견고한 시스템을 획득하고 운영 유지하기 위해 수립하는 계획이다.

대비하기 위한 비용 효율적인 보호대책을 수립하고 실행하는 위험관리 프로세스이다.

〈표 1〉 PPP 보호대상 별 주요 내용

	기술	구성품	정보
목적	CPI의 침해 및 유출 방지	핵심 구성품의 취약성 및 악성 행위 방지	프로그램, 체계의 정보 유출 방지
보호 활동 예	- 안티탬퍼 - 수출통제	- 소프트웨어 보증 - 하드웨어 보증 - 신뢰 파운드리 - 공급망 위험관리	- 정보 분류 - 정보보호 - 수출통제

1) 기술(technology)은 기술적 우위에 기여하는 능력으로 이를 CPI(Critical Program Information)로 식별한다. CPI의 보호를 위한 활동으로 안티탬퍼, 수출통제 등이 있으며, 본 논문의 연구주제와 밀접한 관련이 있다.

2) 구성품(component)은 핵심 임무 기능이 구현되는 핵심 구성품을 하드웨어, 소프트웨어, 펌웨어 수준에서 식별하고 보호하는 것이다. 구성품 보호는 구성품에 설계상 취약성이 없도록 보증하고 공급망을 통한 악성 기능이 포함되지 않도록 보증하는 것으로 소프트웨어 보증(assurance), 하드웨어 보증 및 신뢰 파운드리(trusted foundry), 공급망 위험 관리(supplychain risk management) 등의 보호 활동이 있다.

3) 정보(information)는 획득 프로그램 및 획득 대상체계의 정보 등을 보호하는 것으로, 정보 분류와 정보보호, 수출통제 등의 보호 활동이 있다. 우리나라의 군과 방산업체 등에서 수행하는 기밀분류, 문서보안, 인원보안, 시설보안, 정보통신보안 등이 해당된다.

프로그램 보호를 위해 수행할 주요 활동은 다음과 같다. 획득절차의 주요 단계마다 이 활동을 반복적으로 수행하면서 PPP 문서도 최신화한다.

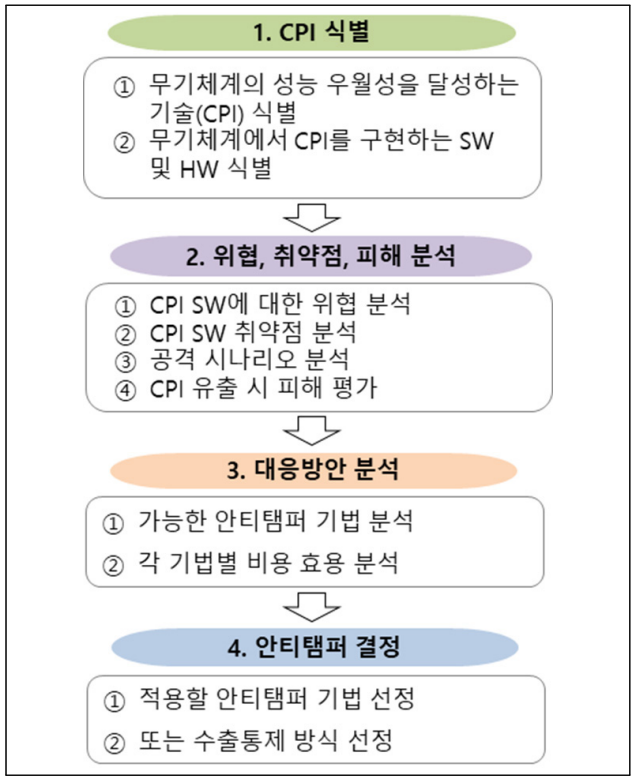
1) 보호대상 (CPI, 핵심 구성품, 정보) 식별
2) 위험평가
3) 보호대책 수립
4) 보호대책 구현
5) 평가 및 감독

보호대책은 〈표 1〉의 보호활동에 기술된 것이며 모든 보호대책을 적용하는 것이 아니라 구현 비용, 효과 등을 분석하여 비용 효율적인 보호대책을 결정하게 된다.

안티탬퍼링 적용 여부는 PPP의 활동에서 결정된다. 본 연구는 위 PPP의 활동 중에서 안티탬퍼링 보호대책이 수립되기까지의 절차에 중점을 두고 있다. 즉, PPP 활동을 통해 보호대상인 CPI가 식별되고 CPI의 취약성 및 위협 분석을 통한 위험평가를 수행하고나면 CPI의 보호를 위한 여러 보호대책이 검토된다. 이때 안티탬퍼링 기술 구현시 발생하는 비용, 일정, 성능 영향도 등과의 절충 분석을 통해 안티탬퍼링 적용 여부를 결정하게 된다.

2.2. 안티탬퍼링 프로세스

안티탬퍼링은 무기체계에 구현된 기술의 역설계를 억제, 지연, 감지 및 반응하기 위한 공학적 보호대책이다. 안티탬퍼링 프로세스는 독립적으로 존재하는 것이 아니라 프로그램 보호 계획인 PPP 프로세스에 의해 수행되지만, 안티탬퍼링 관점에서 도식화하면 〈그림 2〉와 같다.



〈그림 2〉 안티탬퍼링 프로세스

안티탬퍼링 결정 프로세스의 주요 내용은 다음과 같다.

1) CPI 식별
2) 위협·취약성 분석을 통한 위험평가
   - 위협 및 취약성 분석
   - 공격 시나리오 식별과 피해 평가
3) 대응방안 분석
   - 적용 가능한 안티탬퍼링 기술 식별
   - 각 기술별 타당성 분석(비용, 일정, 성능 등)
4) 안티탬퍼 결정
   - 안티탬퍼 적용이 어려운 경우, 수출통제 방식을 선정하여 기술을 보호함

미국 획득체계의 각 검토 단계에서 수행되는 안티탬퍼링 활동을 요약하면 〈표 2〉와 같다[2].

〈표 2〉 검토단계별 안티탬퍼링 활동

단계	안티탬퍼링 활동
ASR	- 체계 성능에 대해 AT 요구사항 분석 - AT 개념 정립
SRR	- 체계 성능에 대해 AT 요구사항 갱신
SFR	- 체계 기능 기준선에 대해 AT 요구사항 갱신
PDR	- 할당 기준선에 대해 AT 요구사항 갱신 - AT 계획서 초안 완성
CDR	- 제품 기준선에 대해 AT 요구사항 확정 - AT 구현 비용과 남는 취약성 분석 - AT 평가 계획 수립 - AT 계획서 최종안 완성
SVR/FCA	- AT 평가

〈표 2〉에서 보듯이 획득 초기 단계부터 안티탬퍼 요구사항을 분석하면서 안티탬퍼링 적용여부를 결정하게 되며, CDR 시점에 AT 계획서를 완성한다.

2.3 분석 및 시사점

국내는 무기체계 획득 프로그램 보호 제도가 없으며, 미국의 프로그램 보호에서 다루는 일부가 운용되고 있다. 미국 프로그램 보호의 3요소에 대해 국내 제도를 비교하면 〈표 3〉과 같이 요약된다.

〈표 3〉 미 프로그램 보호와 국내 제도 비교

PPP 요소	국내 제도
정보	- 군사기밀: 국방보안업무훈령, 방산보안업무훈령 등으로 보호 - 기밀은 아니지만 보호할 정보: 분류 및 보호에 대한 관련 법령 부재
기술	- 방산기술보호법, 방산기술보호지침 시행 - 국과연/방산업체는 방산기술 식별 및 보호 제도 시행 - 무기체계 연구개발에 안티탬퍼링 기술 적용 예정 - 안티탬퍼링 프로세스 지침 부재
구성품	- 핵심 구성품 식별 및 관리 제도 부재 - 소프트웨어 신뢰성/보안성 검증 운용 중 - 소프트웨어 보증 제도 미흡 - 하드웨어 보증 제도 부재 - 공급망 보안 제도 부재

안티탬퍼링 프로세스와 관련하여 분석된 시사점은 다음과 같다.

첫째, 미 국방부의 안티탬퍼링 프로세스는 체계공학적 방법론에 기반하여 기술검토회의 시점마다 최신화하고 검토받고 있다. 국내의 연구개발도 미국과 유사한 체계공학 방법론을 적용하고 있으며 [17-18], 체계공학에 기반한 안티탬퍼링 프로세스를 개발하는 것이 필요하다.

둘째, 국내 안티탬퍼링 프로세스의 도입을 위한 방법으로 미국과 같은 프로그램 보호 제도를 도입한 후 시행하는 방법과 프로그램 보호 제도와는 무관하게 안티탬퍼링 프로세스를 우선 시행하는 방법이 있을 수 있다. 방산업체 및 국과연에서 안티탬퍼링 기술을 적용하는 연구개발 사업이 진행될 예정이므로 안티탬퍼링 프로세스를 프로그램 보호 제도보다 먼저 시행하되, 보호대상의 식별부터 보호대책의 결정까지의 안티탬퍼링 프로세스를 활용하여 프로그램 보호 제도를 정립해나가는 것이 바람직하다.

셋째, 미 국방부의 프로그램 보호, 안티탬퍼링 관련 규정/지침들은 최상위 이해관계자가 활용할 수 있는 프로세스 위주로 기술되어 있고 자세한 지침은 찾기 어렵다. 특히 무기체계 안티탬퍼링 기술에 대해서는 비밀로 보호하고 공개하지 않고 있어 자체적인 연구개발이 필요하다.

주2) ASR(Alternative System Review), SRR(System Requirement Review), SFR(System Functional Review), PDR(Preliminary Design Review), CDR(Critical Design Review), SVR(System Verification Review), FCA(Functional Configuration Audit)

Ⅲ. 제안 방안

3.1. 안티탬퍼링 프로세스 개요

무기체계 연구개발간 수행하는 체계공학적 절차에서 안티탬퍼링 (AT) 개발 절차를 〈표 4〉와 같이 8개 과정으로 정의하고 이를 크게 3단계 활동으로 구분하였다.

〈표 4〉 AT 개발 및 주요 절차

무기체계 개발 절차		AT 개발 절차	주요 활동
체계 요구사항 분석	SRR	① AT 요구사항 분석	'계획수립' 단계
체계 구조설계	SFR	② 보호(기술) 식별 ③ 보호 대책 식별	① AT 요구분석 ② 방산기술 식별 [②,④,⑤,⑥ 반복] ⇓ [위험평가(기술평가)] ⇓ ③ AT 기법(구체화) [②번 항으로 반복]
기능/성능 요구분석	SSR	④ 형상 품목 식별	
구조설계	PDR	⑤ HW/SW 구성품 식별	
상세설계	CDR	⑥ 하위구성품 식별	
개발/체계 통합	TRR	⑦ 구현(개발) 및 통합시험	'개발/통합' 단계
시험평가 /규격화		⑧ 시험평가 및 규격화	'평가/규격화' 단계

본 연구에서는 위 주요 활동 중 첫 번째인 계획수립 단계 중 'AT 요구사항 분석, 방산기술 식별, 위험평가' 절차에 한정하여 연구하였다.

3.2 안티탬퍼링 요구사항 분석

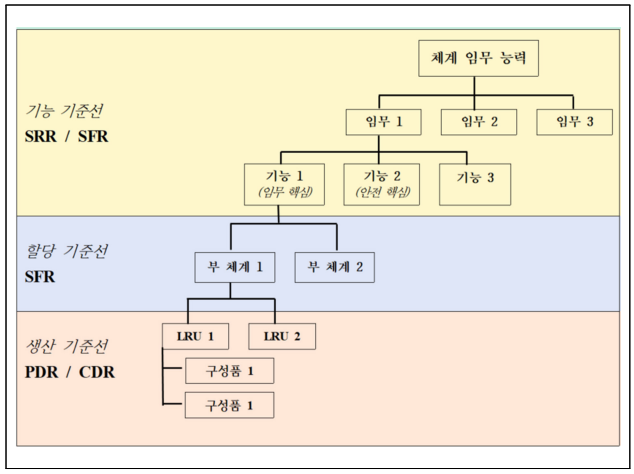
무기체계 연구개발 프로세스 중에서 가장 먼저 진행되는 체계요구사항 분석(SRR)을 준비하며 AT 요구사항을 식별하고 정의해야 한다.

AT 요구사항 분석 및 정의는 AT 적용 대상 기술과 보호해야 할 대응 수준을 결정하는 중요한 절차이다.

AT 요구사항은 최초 선행연구부터 식별할 수 있으나 소요군의 작전요구성능(Required Operational Capability: ROC)이 AT 요구사항의 근거가 되는 것이 좋다. 방위사업청의 통합 프로젝트 관리팀(IPT)은 ROC에 근거하여 군의 보안 관련기관에게 'AT 요구'를 포함한 '보안요구사항 정의'를 의뢰하고, 결과를 제안요청서로 작성하여 연구개발 기관에게 요구하는 것이 바람직한 방법(절차)으로 판단된다. 연구개발 기관은 'AT 요구사항 정의서'를 기초로 'AT 요구사항 명세서'를 작성하여 SRR 검토회의의 기초자료로 제공한다.

3.3 방산기술 식별

본 절에서 방산기술의 식별은 AT를 적용해야 할 보호 대상 기술을 식별하는 것으로, 무기체계에 적용될 하드웨어 및 소프트웨어 기술을 구성품 수준으로 식별해야 한다.이를 위해 무기체계 연구개발간 체계공학 절차를 통해 설계를 수행하면서 보호할 방산기술을 구성품 수준으로 식별한다.



〈그림 3〉 체계공학 절차 기반 기능 분해

〈그림 3〉은 무기체계 요구능력에서 임무(mission)를 분석하고 임무를 수행할 기능(function)과 기능을 담당할 부체계(sub-system), LRU(Line Replacement Unit)/구성품까지 설계하는 과정을 설계검토(SRR, SFR, SSR, PDR, CDR) 단계별로 보여주고 있다.

이와같이 체계공학적 설계가 진행될 때 〈표 5〉와 같은 평가항목을 고려하여 보호가 필요한 방산기술을 식별하고 방산기술이 포함된 구성품을 식별한다. 구체적인 평가항목과 평가방법은 무기체계와 사업에 따라 절충하여 결정한다.

〈표 5〉 방산기술 식별을 위한 평가항목

구분		평가항목
① 개념분석	사용자 관점에서 요구수준 관련	□ 외교적 피해 유발 □ 적대국 관련 □ 유출시 영향 □ 역량개발에 도움 □ 타 국가 관심도 □ 체계/운용조직 노출
② 재료분석	체계 재료 및 SW의 추가 보호 필요성	□ 상당한 혁신 수준 □ 알고리즘 추가개발 □ 발전된 능력제공 □ 전략 / 희귀 물자
③ 설계분석	기술적 이점, 유출시 능력의 유출 여부	□ HW 개발 어려움 □ 유출시 위협 유무 □ 타 체계에 영향 □ SW 개발 어려움 □ 유출시 기술이전 가능성 □ 체계 취약성 노출
④ 제조분석	'제조, 공정, 코딩'에 추가 보호 필요성	□ 표준 / 공개 여부 □ 기밀(비공개) 여부 □ 고유 도구/재료 노출 □ 국가이익 저해
⑤ 통합분석	체계통합시 향상된 기능제공 여부	□ 상당한 투자 필요 □ 상용/타국 체계 비교 □ 향상된 능력제공 □ 통합시 취약성 노출
⑥ 운영환경	운영환경에 추가 보호 대책 필요성	□ 유출시 적 능력향상 □ 적의 개발을 가속 □ 유출시 적 EA 가능성 □ 상호운용성 피해

〈표 6〉은 식별된 방산기술(구성품) 목록의 예시로서 위에서 언급한 기능적 분해 작업을 통해 식별된 결과를 보여주고 있다.

〈표 6〉 방산기술(구성품) 식별 목록

	임무 1											임무 2			
	부 체계 1			부 체계 2								부 체계 3			
	LRU 1			LRU 2		LRU 3		LRU 4			LRU 3		LRU 5		LRU 3
구성품	1	2	3	4	5	6	7	4	5	8	3	9	6	7	10	3
000-00-000		0					0					0				0
000-01-000	0							0						0		
000-02-000			0							0						
000-04-000				0					0						0	

또한, 식별된 방산기술은 방산기술보호지침에서 규정하고 있는 관리대상기술 대장에 기록하여 관리한다. 관리대장에는 기술명, 기술명세, 보호종류, 체계명 또는 사업명, 관련구성품, 기술보유기관 등이 기록된다.

다른 사업(체계)에서 식별된 방산기술이 본 사업에서 사용된다면 동일수준으로 보호해야 하며, 방위사업청은 기술 식별 및 보호수준이 방위사업 전체에 일관되도록 보장하는 수평적인 보호 체계를 구축해야 한다.

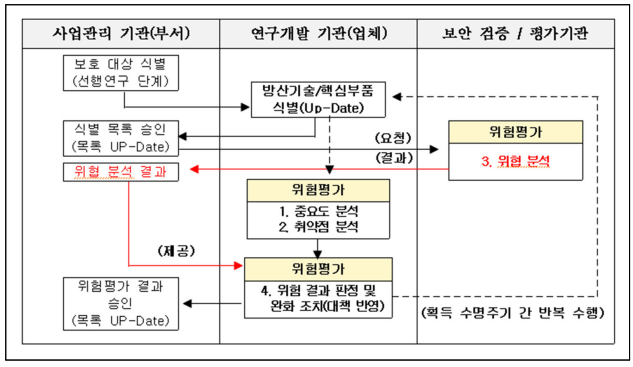
식별 결과는 획득단계별 기술 검토회의 산출물로 작성하여 IPT의 최종 승인을 받는다.

3.4 위험평가

위험평가는 식별된 방산기술에 대하여 어떤 취약성이 어느 수준으로 있고 그 취약성을 완화시키기 위해서는 어떤 조치가 필요한지를 분석해서 AT 대응 방법 및 대응 수준을 결정하기 위해 수행한다.

위험평가는 〈그림 4〉와 같이 중요도 분석, 취약성 분석, 위협 분석의 활동으로 수행되며, 이 중에서 위협 분석은 보안 검증/평가 기관에서 지원할 것을 제안하였다.

1) 중요도 분석은 식별된 방산기술(특정 구성품)이 무기체계의 임무 수행이나 기능 발휘에 얼마나 중요한 역할을 하고 있는지를 평가하는 것으로서 중요도 수준을 1~5 척도(미미한 영향-심각한 영향)로 평가한다.



〈그림 4〉 위험평가 절차도

2) 취약성 분석은 방산기술이 가지고 있는 취약성의 심각도를 분석하는 것으로, 위협으로 인해 체계의 임무 목표를 무력화하거나 성능이 저하될 수 있는 시스템 설계, 개발, 생산, 또는 운영상의 약점을 평가하는데, 취약성 수준을 1~5 척도(미미한 영향-심각한 영향)로 평가한다.

중요도와 취약성 분석 결과를 사용하여 위험 결과

(Consequence)를 산정하며 〈표 7〉과 같이 매트릭스로 표현할 수 있다. 예를 들어, 중요도가 4점, 취약성이 3점으로 평가되었다면 위험 결과는 3점으로 평가된다.

〈표 7〉 위험 결과(Consequence) 평가 매트릭스

위험 결과(Consequence)						
취약성 심각도	5	2	3	4	5	5
	4	2	3	3	4	5
	3	1	2	3	4	5
	2	1	1	2	3	4
	1	1	1	1	2	3
		1	2	3	4	5
	중요도(CA)					

3) 위협분석은 방사청 IPT를 통해 보안 검증/평가 기관 또는 정보기관에 위협분석 요청을 하여 분석 결과보고서를 얻는다. 미 국방정보국(Defense Intelligence Agency)과 같은 정보기관이 위협분석을 담당하며, 사업관리부서의 요청에 따라 위협분석 보고서를 작성하여 제공한다. 위협분석은 위협이 발생할 가능성, 위협이 성공할 가능성을 분석하여 위협 가능성(likelihood)을 평가한다. 위협 발생 가능성은 취약성 평가를 기초로 적의 공격 가능성을 추정하는 것이며, 위협 성공 가능성은 취약성 평가를 기초로 적의 공격이 성공하는데 필요한 비용, 시간. 기법을 고려하여 적의 능력을 추정하는 것이다. 위협 분석은 위협 발생/성공 가능성을 각각 1~5 척도(매우 낮음-매우 높음)로 평가한다.

위협분석 결과를 사용하여 위협 가능성(Likelihood)을 산정하며 〈표 8〉과 같이 매트릭스로 표현할 수 있다.

〈표 8〉 위험 가능성(Likelihood) 평가 매트릭스

위협 가능성(Likelihood)						
위협 발생 가능성	5	2	3	4	5	5
	4	2	3	3	4	5
	3	1	2	3	4	5
	2	1	1	2	3	4
	1	1	1	1	2	3
		1	2	3	4	5
	위협 성공 가능성					

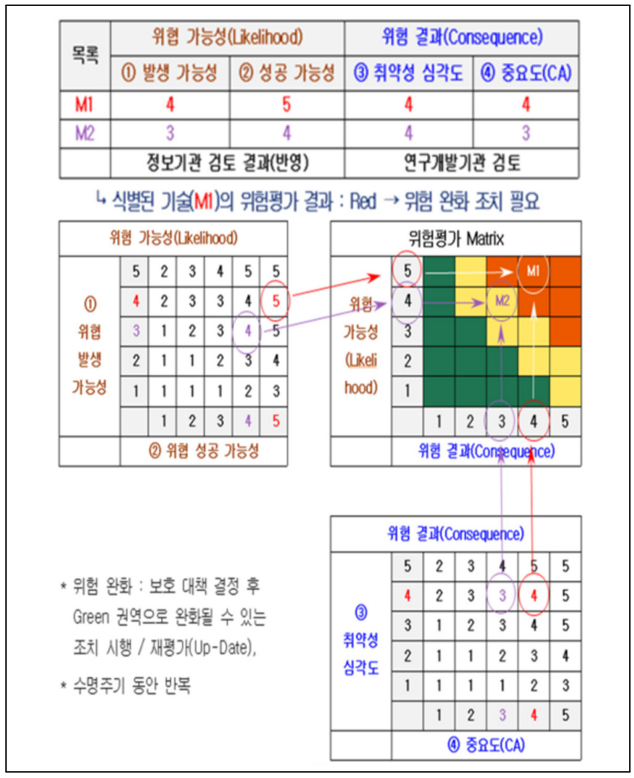
최종적으로 위험 결과 및 위험 가능성 분석 결과를 사용하여 위험을 평가하며 〈표 9〉와 같이 매트릭스로 표현할 수 있다.

〈표 9〉 위험평가 매트릭스

위험평가 Matrix						
위험 가능성 (Likelihood)	5	G	Y	R	R	R
	4	G	Y	Y	R	R
	3	G	G	Y	Y	R
	2	G	G	G	Y	Y
	1	G	G	G	G	Y
		1	2	3	4	5
	위험 결과(Consequence)					

이러한 위험평가는 각 방산기술에 대해 수행한다. 위험평가 결과 빨간색(R) 영역일 경우 위험 수준이 높아 AT 적용이 필요한 기술로 평가하고, 노란색(Y), 초록색(G) 영역일 경우 위험 수준이 낮아 AT 적용이 불필요한 것으로 분류한다.

〈그림 5〉는 제안한 위험평가의 예시를 보여주고 있다. 식별된 방산기술 M1과 M2에 대해 위험평가를 수행하였고, 기술 M1은 위험 결과는 4, 위험 가능성은 5로 평가되어 위험 수준이 R 영역으로 평가되었고 AT 적용이 요구된다. 반면에 기술 M2는 위험 수준이 Y 영역으로 평가되어 AT 적용이 필요하지 않다.



〈그림 5〉 위험평가의 사례

Ⅳ. 결론

국방 선진국은 자국의 국방기술 및 산업기술의 보호를 위해 총력을 기울이고 있다. 미국은 획득 프로그램 보호 제도를 운용하고 있으며, 이를 통해 정부의 획득 조직, 방산업체 조직 및 군수품에 대한 보호체계를 구축하고 적의 위협으로부터 기술, 구성품, 정보를 보호하고 있다. 또한, 미국은 세계 1위의 무기수출 국가로서 자국의 무기체계를 수입한 국가에서 무기체계의 역설계를 통해 기술이 유출되지 않도록 안티탬퍼링 제도를 운용하고 있다.

우리나라 방산물자 수출이 크게 증가하고 있으며 수출용 무기체계의 기술보호를 위해 안티탬퍼링 적용이 요구되고 있으나 아직까지 안티탬퍼링 지침과 제도가 없는 실정이다. 본 연구에서는 체계공학 기반의 안티탬퍼링 프로세스를 제안하고, 안티탬퍼링 프로세스 중에서 앞 단계인 방산기술 식별과 안티탬퍼링 적용 여부를 결정하는 위험평가 방안을 제안하였다. 연구를 위해 국방 선진국인 미국의 안티탬퍼링 관련 지침을 분석하여 국내 획득절차에 적용하였다. 제안한 방안은 방위사업청 및 연구개발기관이 무기체계 획득과 연구개발 절차에서 사용할 안티탬퍼링 지침의 개발에 활용할 수 있다.

방위사업청이 최근 개정한 방산기술보호지침은 무기체계 연구개발 시 방산기술을 식별하고 안티탬퍼링 적용을 명시하고 있다. 그러나, 현행 방산기술보호지침은 안티탬퍼링 적용을 위한 구체적인 내용이 부재하여 방산업체 등 연구개발기관에서는 구체적인 시행이 어려운 실정이다. 현 실정을 개선하기 위해 두 가지 정책을 제안한다.

첫째, 안티탬퍼링 운용 및 지원을 위한 제도를 수립하고 전문기관을 설치하여야 한다. 현재 국방사이버안보훈령에 의해 군사안보지원사령부가 무기체계의 사이버안보를 위한 역할을 담당하고 있으며, 방위사업청은 무기체계의 사이버 보안을 위한 보호대책서를 수립할 때 군사안보지원사령부에 검토받아야 한다. 이와 유사하게 무기체계 안티탬퍼링 기술 및 프로세스 전문가로 구성된 전문기관이 필요하며, 방위사업청 및 연구개발기관의 기술 식별과 위험평가 등의 안티탬퍼링 업무를 수행할 때 전문기관이 지원하여야 한다.

둘째, 안티탬퍼링 기술의 연구개발이 필요하다. 안티탬퍼링 기술은 역설계 시도의 감지 기술, 감지 시의 데이터 소거와 같은 반응 기술, 역설계 억제 및 방지 기술 등이 알려져 있으나 선진국에서는 구체적인 내용을 비밀로 보호하고 있어 국내 자체 개발이 필요하다. 이를 위해 방위사업청은 안티탬퍼링 관련 연구개발 사업을 기획하고 방산업체가 사용할 수 있는 공통 기술로 발전시켜야 한다.

본 연구의 한계점으로는 제안한 기술 식별과 위험평가 방안을 실제 무기체계 개발 사업에 적용하지 못하고 이론적인 연구를 한 점이다. 따라서, 본 논문에서 다루지 않은 안티탬퍼링 프로세스의 각 활동들을 심도있게 연구하여 프로세스를 정립하는 한편 이를 실제 무기체계 연구개발 사업에 적용하는 사례 연구가 필요하다.

참고문헌

1) 방위사업청 훈령, 방위산업기술보호지침, 2020.
2) 이민우, 이재천, “무기 시스템 개발에서 기술보호를 위한 위험관리 기반의 Anti-tampering 적용 기법”, 한국산학기술학회 논문지, 제19권 제12호, 2018.
3) 이민우, “국방 무기시스템 기술보호를 위한 수명주기 프로세스 모델 개발”, 아주대학교 박사학위논문, 2019.
4) Lt Col Arthur F. Huber, et al, “The Role and Nature of Anti-tamper Techniques in US Defense Acquisition”, Acquisition Review Quarterly, Fall 1999.
5) DoDD 5200.47E, “Anti-Tamper (AT)”, September, 2015.
6) US General Accounting Office Report GAO-04-302, “Defense acquisitions : DoDneeds to better support program manager’s implementation of anti-tamper protection”, 2004.
7) DoD“Program Protection Plan Outline & Guidance”, July, 2011.
8) DoDI 5200.39, “Critical Program Information (CPI) Identification and Protection within Research, Development, Test, and Evaluation (RDT&E)”, May, 2015.
9) DoDI 5200.39, “Required Use of Standardized Process for the Identification of Critical Program Information (CPI) in DON Acquisition Programs”, September, 2007.
10) DoDI 5200.44, “Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)”, November, 2012.
11) DoDI 8510.01, “Risk Management Framework (RMF) for DoD Information Technology”, March, 2014.
12) USAF “Weapon System Program Protection / System Security Engineering Guidebook”, Version 2.0, March, 2020.
13) Malinda Reed, “System Security Engineering and Program Protection Integration into SE”, 17th Annual NDIA Systems Engineering Conference, October, 2014.
14) Malinda Reed, “Systems Engineering Requirements Analysis and Trade-off for Trusted Systems and Networks Tutorial”, March, 2013.
15) Raymond Shanahan, “Identification and Protection of Critical Program Information (CPI)”, 18th Annual NDIA Systems Engineering Conference, October, 2015.
16) E. Fong, “Comprehensive Program Protection Planning”, 14th Annual NDIA Systems Engineering Conference, October, 2011.
17) 방위사업청, SE 기반 기술검토회의 가이드북, 2017.
18) 방위사업청, SE 기반 위험관리 가이드북, 2018.