Journal of the Korea Academia-Industrial cooperation Society
Vol. 19, No. 12 pp. 99-109, 2018

https://doi.org/10.5762/KAIS.2018.19.12.99
ISSN 1975-4701 / eISSN 2288-4688

무기 시스템 개발에서 기술보호를 위한 위험관리 기반의 Anti-Tampering 적용 기법

이민우, 이재천*
아주대학교 시스템공학과

Risk Management-Based Application of Anti-Tampering Methods in Weapon Systems Development

Min-Woo Lee, Jae-Chon Lee*
Dept. of Systems Engineering, Ajou University

요 약 기술적으로 보호된 시스템으로부터 역공학 등을 통해 기술을 불법으로 도출하거나, 도출된 기술을 무단으로 사용하여 시스템 개발에 사용하는 것을 Tampering이라고 하며, 특히 무기 시스템에 대한 Tampering은 안보에 위협이 된다. 따라서 이를 방지하기 위해 Anti-tampering이 필요한데, 선행연구로서 Anti-tampering의 필요성과 관련 동향, 적용 사례가 발표되었으며, Cybersecurity 기반의 접근 또는 더욱 강력한 소프트웨어 보호기법에 대한 연구들이 수행되고 있다. 국내에서는 방산기술보호법에서 유관기관에서 인력, 시설, 정보체계를 통한 기술유출을 방지하기 위한 활동에만 초점이 맞추어져 있고, Anti-tampering을 위한 기술적 활동은 별도로 정의된 바가 없다. 무기 시스템 개발에서 Anti-tampering 설계를 적용하려고 하면, 개발비용 및 일정에 미치는 영향을 고려하여 Tampering으로부터 보호해야 할 기술을 선별할 필요가 있다. 그럼에도 불구하고 기존 연구에서는 국내실정을 반영한 관련 연구가 없어 무기 시스템에 대한 기술보호 수행에 어려움이 있다. 이를 해결하기 위해 본 연구에서는 Anti-tampering을 통해 보호가 필요한 대상 기술을 선정하는 방법과 선정된 기술을 보호하기 위한 대응기법의 결정 방법을 연구하였다. 구체적으로, Anti-tampering 적용을 위한 적절한 검토시점 및 주체를 제시하고, 보호대상 기술을 선정하기 위한 방법으로 위험분석 개념을 적용한 평가 행렬을 도출하였다. 또한, 위험완화 개념을 기반으로 Anti-tampering 기법들을 적용 가능성으로 분류하고 또한 적용 수준을 판단하는 방법을 연구하였다. 연구결과를 적용하여 사례분석을 수행한 결과, 무기 시스템에서 어떤 요소기술에 대해 보호기법을 적용하는 것이 필요한지, 그 경우에 어떤 수준의 적용이 필요한지에 대해 체계적으로 평가할 수 있었다. 향후 무기 시스템의 전수명주기적 관점에서 Anti-tampering 프로세스 연구로의 확장이 필요하다.

Abstract Tampering involves illegally removing technologies from a protected system through reverse engineering or developing a system without proper authorization. As tampering of a weapon system is a threat to national security, anti-tampering measures are required. Precedent studies on anti-tampering have discussed the necessity, related trends, application cases, and recent cybersecurity-based or other protection methods. In a domestic situation, the Defense Technology Protection Act focuses on how to prevent technology leakage occurring in related organizations through personnel, facilities and information systems. Anti-tampering design needs to determine which technologies are protected while considering the effects of development cost and schedule. The objective of our study is to develop methods of how to select target technologies and determine counter-measures to protect these technologies. Specifically, an evaluation matrix was derived based on the risk analysis concept to select the protection of target technologies. Also, based on the concept of risk mitigation, the classification of anti-tampering techniques was performed according to its applicability and determination of application levels. Results of the case study revealed that the methods proposed can be systematically applied for anti-tampering in weapon system development.

Keywords : Anti-Tampering, Technology Protection, Systems Engineering, Weapon Systems, Risk Management

*Corresponding Author : Jae-Chon Lee(Ajou Univ.)
Tel: +82-31-219-3941 email: jaelee@ajou.ac.kr
Received September 17, 2018 Revised (1st October 1, 2018, 2nd October 18, 2018)
Accepted December 7, 2018 Published December 31, 2018

1. 서론

지식재산권과 관련된 오랜 연구와 더불어, 최근 국내 방산분야에서도 기술유출 사례가 증가하고 있다[1]. 무기 시스템에 적용된 핵심기술을 역설계 등을 통해 유출하거나, 이 기술을 무단 변경하여 무기 시스템 복제 또는 대응수단 개발에 사용하는 행위를 Tampering이라고 하는데, 이는 그 기술을 개발한 많은 노력을 사장시킴과 동시에 경제적인 손실과 국가안보에 대한 위협으로 작용한다. 따라서 우리는 무기 시스템으로부터 중요기술이 유출될 가능성에 대비해야 한다.

미국은 중요기술 유출을 방지 또는 지연시키기 위한 여러 가지 정책을 시행하고 있다. 이 중 무기 시스템에 적용되는 것이 Anti-Tampering이며, 이는 무기 시스템의 기술을 보호하기 위한 활동으로서, 중요기술에 대한 비인가자의 접근을 차단 또는 지연시켜 기술유출에 대비하는 것이다[2].

Anti-Tampering과 관련된 기존의 연구들은 관련동향 및 필요성을 논의하거나, 구체적 접근으로서 H/W 및 S/W 분야의 더욱 강한 보호기법에 대한 연구들이 주를 이루고 있다[3-6]. 선행연구만으로 우리나라에 Anti-Tampering을 적용하기 위해 활용하기는 다소 어렵다고 할 수 있다.

한편, Anti-Tampering을 통해 무기 시스템의 모든 요소기술을 보호할 수는 없을 뿐만 아니라, 애당초 그러한 행위 자체는 불필요하다. 이는 보호기법을 적용할 시 무기 시스템의 개발비용이 증가하거나 개발 일정이 지연될 뿐만 아니라, 시스템 운용자의 정비작업에도 상당한 영향이 예상되기 때문이다. 따라서 보호해야만 하는 대상기술이 무엇인지를 식별하여 무기 시스템 개발과정에 반영할 수 있는 검토과정이 필요하다[7-8].

우리나라는 2012년 방위사업청에 방산기술통제관실을 설치하였고, 2015년 「방위산업기술 보호에 관한 법률」을 제정하는 등 나름대로 방위산업분야 기술보호 활동을 수행하고 있다. 그러나 이는 인원통제, 시설 및 정보보호 체계로 구성된 것으로서 정부기관 및 연구개발 수행기관으로부터의 기술자료 유출 및 침해 방지에만 집중된 것이다[9]. 또한, 무기 시스템의 기술보호를 위한 Anti-Tampering에 대한 낮은 인지도와 관련제도의 부재뿐만 아니라 학술적 연구실적 역시 극히 드문 상황이기에, 아직 국내에서는 무기 시스템에 대한 기술보호 수행은 어려움이 있다고 할 수 있다.

본 논문에서는 Anti-Tampering의 적용을 통해 보호해야 할 필요가 있는 기술을 선정하는 방법과 함께, 해당 기술을 보호하기 위해 무기 시스템에 적용할 보호기법을 선정하는 방법을 제시하였다. 먼저, 이러한 활동이 다양한 시점에서 수행되어야 하므로 수행시점과 함께 검토주체를 제시하였다. 또한, '기술유출'은 '위험'으로 간주할 수 있으므로 위험관리 절차 중 '위험분석'을 적용한 Evaluation Matrix를 도출하였고, '위험완화'를 적용하여 평가결과의 활용방법을 제시하였다.

제시한 방법의 유용성을 확인코자 사례분석을 수행한 결과, 다양한 시점에서 무기 시스템의 각 요소기술별로 Anti-Tampering 적용 필요성과 적용수준을 간편하고 체계적으로 검토할 수 있었다.

이어지는 2장에서 Anti-Tampering 적용 필요성, 미국의 관련제도 소개와 함께 연구동향 및 목표를 제시하였다. 3장에서는 위험관리절차를 적용하여 Anti-Tampering 적용대상과 기법을 선정하는 방법을 도출하였고, 4장의 사례분석을 통해 그 유용성을 확인하였다. 마지막으로 5장에서 본 논문의 연구결과를 정리하였다.

2. 문제의 정의

2.1 Anti-Tampering 적용의 필요성

최근 방산업체 자료 유출(2013.10월), 해킹 공격(2015.11월, 2016.4월), 방위사업청 사칭 이메일 발송(2016.5월) 등 기술유출 시도가 증가하고 있다[1]. 이에, 방위사업청은 '산업보안' 개념을 방산분야에 반영하여 2015년 12월 「방위산업기술보호법」 제정을 시작으로 "튼튼한 방위산업기술 보호체계 구축을 통한 국가안전보장 및 국익 제고에 기여"를 추구하는 '방산기술보호' 개념을 정립하고, 기술보호 정책 수립 및 기업의 기술보호활동 감독 및 역량구축 지원 등의 업무를 수행하고 있다[9].

「방위산업기술보호법」 및 같은 법 시행령에서 정의하는 바와 같이, 국방분야에서 기술보호를 위한 활동은 '보호대상기술의 식별・관리', '인원통제 및 시설보호', '정보보호' 등으로 볼 수 있으며, 이는 국방부 및 방사청 등의 정부부처와 국과연・기품원 등 정부출연기관, 방위사업에 참여한 기업들로부터 연구개발사업 수행에 따라 산

출된 기술자료들이 유출되지 않도록 하는 것이라고 볼 수 있다.

그러나 유관기관으로부터의 기술유출을 완벽히 차단하였다고 하더라도 무기 시스템 자체로부터의 기술유출 가능성이 존재하기에, 별도의 대응방안이 필요하다. 무기 시스템 분야에서 선도적인 역할을 하는 미국조차도 무기 시스템을 통한 기술유출에 완벽히 대처할 수 없었으며, 실제로 유·무인기가 운용 도중 중국, 이란에 나포되어 역설계된 것으로 평가되는 등의 기술유출 사례가 있었다[3-4].

Table 1의 시나리오와 같이 다양한 경로로 무기시스템으로부터 기술이 유출될 수 있다. 이는 수많은 개발자들이 험난한 연구개발과정을 수행하며 쏟은 열정과 피땀 어린 노력을 수포로 만들 뿐만 아니라, 무기 시스템의 핵심기술이 고스란히 적성국가 및 테러단체로 이전(移轉)되어 국가안보를 위협하는 결과로 이어지므로 이에 대한 대비책이 필요하다.

Table 1. Leakage scenario and result by weapon itself

Intention	Leakage scenario	Result
Intended	· Stolen by hostile · Re-export to third party (countries, companies, etc.)	· Modification · Reverse - engineering · Counter - measures developed
Not intended	· Lost(Control errors or Malfunction) · Guided weapon has unexploded	

무기 시스템으로부터 기술유출을 방지하기 위한 공학적 조치로 Anti-Tampering이 있다. 미 국방성은 Anti-Tampering에 대해 “비의도적 기술이전 또는 역설계로 인한 시스템 변경 및 대응수단(Counter-measures)이 개발되는 것을 막기 위해 국내운용 및 수출 시 무기 시스템으로부터 CPI(Critical Program Information) 유출을 방지 또는 지연시키는 시스템 엔지니어링 활동”이라고 정의하고 있다[2].

국내에서는 이를 “기술보호기법”[3] 또는 “부당변경 방지”[4] 등으로 번역하고 있으나, 아직 공식적인 표현이 존재하지 않으므로 본 논문에서는 원어를 그대로 사용하도록 하겠다.

Anti-Tampering은 H/W분야와 S/W분야의 다양한 기법들을 포함하는데, 일반적으로 요구목적에 따라 억제(Deterrence), 감지(Detection), 방지(Resistance), 반응(Response) 등으로 분류할 수 있다[3-4].

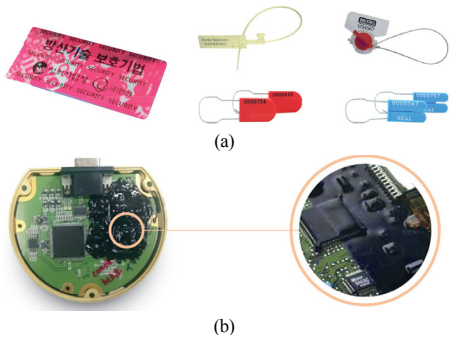


Fig. 1. Examples of Anti-Tampering technique[4]
(a) Tamper indicating devices(Seal & Labels)
(b) Coating(Encapsulation materials)

2.2 미국의 기술보호제도 및 절차

미국은 CPI를 보호하기 위해 우리나라의 방산기술보호 개념, 즉 유관기관으로부터의 기술유출 방지뿐만 아니라, 사이버보안과 Anti-Tampering 등 제반분야를 망라한 계획인 PPP(Program Protection Plan)를 수립하고, 무기 시스템의 수명주기 전반에 걸쳐 관리하고 있다[10]. 또한, 불필요한 예산낭비 방지 및 사업관리의 효율성 제고를 위해 PPP를 통해 보호해야 할 CPI를 선정·관리하고 있다[10].

Anti-Tampering 분야의 경우, 1999년 미 국방부 획득기술군수실(AT&L)에서 정책을 선포한 이후 2001년 EA(Executive Agent), 즉 이행부서로 공군을 지정하였고, 이에 따라 미 공군연구소를 중심으로 정책이행과 기술개발 및 관리, 유관부서 교육 등의 업무를 수행하고 있다[8]. Anti-Tampering은 PPP와 마찬가지로 획득주기 전반에 걸쳐 수행되는데, 4개의 EP(Evaluation Points)를 통해 획득순기별로 검토를 수행한다. EP1(MS-A, AT Concept) 시 기술적 분석과 초기비용 예측을 수행하며, EP2(MS-B/PDR, AT Plan)에서 CPI를 최신화하고 보호기법을 검토한다. EP3(CDR AT Plan / CDR AT V&V Procedures) 시 구현 및 검증방안이 구체화되고, EP4(MS-C, AT V&V Report)에서는 Anti-Tampering이 적절히 구현되었는지를 확인한다[10].

2.3 관련 선행연구

Anti-Tampering의 경우, 이행 프로세스에 대한 학술

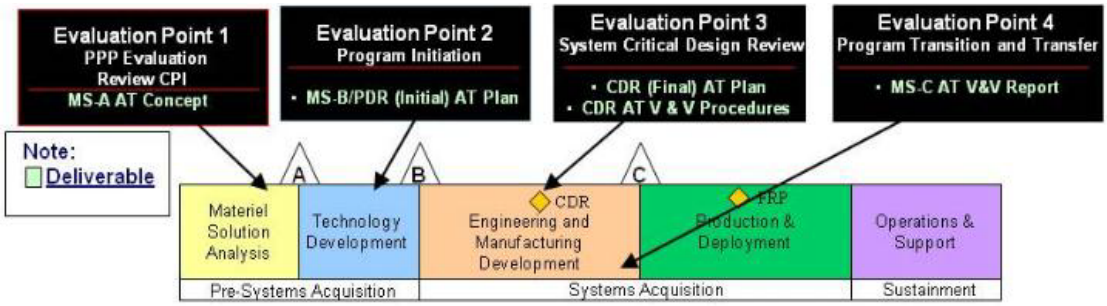


Fig. 2. Anti-Tamper Evaluation Points(EP) for Programs[10]

적 연구는 미비하며, H/W 및 S/W 분야별로 기술적 보호기법 동향을 분석하거나[5], 세부적인 접근으로서 더욱 강한 보호기법의 개발을 소재로 하는 연구가 있다[6]. 한편, 기존 절차를 바탕으로 최근 중요성이 부각되고 있는 사이버보안 분야와의 통합에 대한 연구가 존재한다[11].

우리나라의 경우, 아직 관련분야의 제도와 연구 실적이 미비한 편이다. 현재 연구개발 프로세스는 Anti-Tampering 관련내용을 포함하고 있지 않고, 학술적 연구 역시 그 필요성을 소개하거나[3,12] 미국의 Anti-Tampering 적용절차 중 일부를 활용, 연구개발주관기관의 입장에서 각각의 보호기법을 적용한 사례에 대해 소개하는 수준에 머물러 있다[4,12]. 따라서 우리나라 연구개발사업의 특성에 맞는 Anti-Tampering 절차를 수립할 필요가 있다.

한편, 미 회계감사국(GAO)은 Anti-Tampering 관련 정책의 효율적인 구현 여부를 감사한 바 있다[7-8]. 2004년의 감사 결과 'Critical technology', 즉 Anti-Tampering을 통해 보호해야 하는 기술이 명확하게 식별되어야 한다는 점과 Anti-Tampering이 비용 및 일정에 미치는 영향이 적지 않다는 점을 식별하였고[7], 이후 2008년의 감사에서도 여전히 동일한 문제점이 식별되어 유관부서 간 유기적인 협업을 위한 이행방안을 권고한 바 있다[8]. 따라서 Anti-Tampering을 통해 보호해야 할 기술을 효율적으로 식별할 수 있는 방안을 마련해야 하며, 적용기법의 수준 역시 비용 및 일정에 미치는 영향을 최소화하기 위해 과도하지 않은 수준으로 통제되어야 한다.

2.4 연구목표 및 범위

무기 시스템의 기술보호와 관련하여, 선행연구를 통해 도출한 본 논문의 연구 목표는 크게 2가지로 분류할 수 있다. 첫 번째로, 무기 시스템에 적용될(또는 적용된) 국방과학기술 중 Anti-Tampering이 필요한 '보호대상 기술'의 식별·선정하는 방법을 확보하는 것이다. 현재의 개발 프로세스 수행 시 추가적인 행정소요를 최소화하는 범위 내에서 제시되어야 할 것이며, 보호대상 기술을 식별·선정하는 주관부서 및 적절한 시점에 대한 검토가 병행되어야 할 것으로 판단된다.

두 번째로, 식별·선정된 '보호대상 기술'에 대해 어떤 종류의 Anti-Tampering 기법을 적용할 것인지, 적용 수준은 어떻게 통제할 것인지 결정하는 방법을 확보하는 것이다. Anti-Tampering 기법은 목적에 따라 다양하게 분류되며, 기능의 흐름을 고려하여 적절한 수준으로 통제될 필요가 있다.

3. Anti-Tampering 적용대상 및 기법의 선정 방법 도출

3.1 연구개발 프로세스 분석을 통한 Anti-Tampering 적용 검토시점과 수행조직의 결정

방위사업, 특히 연구개발사업은 그 프로세스가 다수의 중복된 행정소요를 포함하고 있다는 의견에 따라 기존의 프로세스를 단축시키고자 하는 연구가 상당히 활발하게 이루어지고 있다. 따라서 Anti-Tampering 적용을 통해 보호하여야 할 대상기술이 무엇인지에 대한 검토시점을 별도로 추가하는 것 보다는 현재의 연구개발 프로세스 내에서 검토할 수 있도록 하여 행정소요를 최소화할 필요가 있다. Anti-Tampering 적용 검토시점과 그 검토 수행을 주관하는 조직에 대해 검토해 본 결과, 첫 번

째로 선행연구 조사/분석 수행과정에서 실시하는 TRA (Technical Readiness Assessment, 기술성숙도 평가) 시점에서 합참과 방사청의 협조를 받아 기품원이 주관하여 검토를 수행하고, 두 번째로 탐색개발 최종단계에서 실시하는 TRA 시점이며, 역시 기품원이 주관하는 것이 적절하다. 세 번째로는 개발된 무기시스템의 수출소요 발생에 따라 개조개발을 추진하는 시점인데, 이때는 방사청 방산기술통제관실이 주관하는 것이 적절하다.

왜냐하면, 현재 TRA를 통해 무기 시스템의 핵심기술요소(CTE, Critical Technique Element)를 검토 및 선정하고 각각의 CTE별로 TRL(Technical Readiness Level, 기술성숙도)를 평가하여 적정한 개발단계 선정을 위한 참고자료로 사용되기 때문에 어떠한 요소기술들이 해당 무기 시스템에 적용되는지 쉽게 파악할 수 있기 때문이다. 탐색개발 최종단계에서 체계개발 전환 적절성을 판단할 목적으로 수행하는 TRA의 경우, 선행연구 당시는 보호가 필요하다고 판단했던 기술들이 탐색개발 기간 중 진부기술이 되었거나, 설계과정에서 추가적으로 중요한 기술이 반영되었을 가능성이 있기 때문에, 적절한 시점으로 판단하였다. 이 때, TRA 수행주관이 기품원이므로 기존의 TRA 수행절차 상 보호대상 기술을 검토하는 과정만 추가하면 된다고 본다.

무기 시스템 수출 시, 수출대상국의 기능 및 성능 요구사항을 고려한 기술변경이 수반된다(우리나라 역시 국외구매 사업 시 기술변경을 요구한다). 만약 무기 시스템에 Anti-Tampering이 적용되지 않았다면, 개조개발 수행 초기에 Anti-Tampering 적용여부를 판단하여야 할 것이다. 이 경우, 기존 선행연구의 TRA 결과 또는 체계개발결과보고서 등을 활용하여 비교적 수월하게 평가할 수 있을 것이다. 방위사업청 방산기술통제관실은 무기 시스템의 해외수출 시 검토 및 승인 등의 업무뿐만 아니라, 방위산업기술의 지정·변경·해제 등의 업무까지 수행하고 있으므로 수출소요 발생 시 개조개발 시점에서 가장 적절한 수행기관으로 검토하였다. 다만, 보호대상 기술을 선정하는 업무는 위 기관이 단독으로 수행하는 것이 아니라, 합동참모회의 또는 기술보호심사위원회 등 기존의 의사결정과정을 활용할 수 있도록 하는 것이 타당할 것이다.

3.2 Anti-Tampering 적용 대상기술 선정을 위한 위험관리 절차의 활용 필요성 도출

제시한 시점별로 Anti-Tampering 적용 검토 수행조직이 '어떻게 Anti-Tampering 적용 대상기술을 선정할 것인가'에 대해 검토한 결과, 위험관리(Risk Management)를 최적의 방법론으로 도출하였다.

미 국방성의 "Risk, Issue, Opportunity Management Guide[13]"와 이를 토대로 우리의 방위사업 환경에 알맞게 관련규정 등을 고려하여 작성된 "SE기반 위험관리 가이드북[14]" 에 따르면, 위험관리라는 개념은 프로젝트 수행의 비용/일정/성능에 지장을 줄 수 있는 위험요소를 식별하고 이를 효과적으로 관리하는 방법론으로서 방위사업의 추진과정 내내 유관기관과의 협조를 통해 이행된다[13-14].

Fig. 3. Risk Management Process Overview[13]

Anti-Tampering 적용의 주요 목적인 '기술유출 위험성'이 '위험'의 범주에 포함되는 것으로 볼 수 있기 때문에 Anti-Tampering 관련활동에 위험관리 절차를 적용하는 것은 타당한 것으로 판단된다. 또한, 위험분석(Risk Analysis)은 사업에 영향을 줄 수 있는 위험요소들을 식별하는 초기단계의 절차로서 Anti-Tampering 적용대상 기술 선정과 그 성격이 상당히 유사하기 때문에 이 점에 주목할 필요가 있다.

3.3 Anti-Tampering 적용 대상기술 선정 방법 개발

위험분석은 '영향성(Consequence)' 및 '발생 가능성(Likelihood)'을 양 축으로 작성된 Risk Reporting Matrix 평가결과에 따라 위험요소별 관리수준을 결정한다[13].

Anti-Tampering 적용 대상기술을 선정함에 있어, 양 축은 각각 '기술의 중요도' 및 '기술의 취약성'이 적절할 것이다.

3.3.1 기술의 중요도 및 취약성 판단기준 도출

'기술의 중요도'의 경우, 문자 그대로 해당 기술이 얼마나 중요한 것인지를 나타내는 척도로서 '매우 중요', '중요', '중요도 낮음'으로 구분하였다.

Table 2. Detail measurements about 'The Importance'

Grade	Details
High	· Defense industry tech. (Designated by DAPA) · Latest technology (within 5 years) · Developed as Core tech. R&D projects (technology transfer from abroad is restricted)
Med	· Defense industry tech. (Designated by DAPA) * Technological obsolescence is expected · Not yet fully developed in the country of pursuit (within 10 years)
Low	· Commercial-based tech. · Already available in most countries

'기술의 취약성'의 경우, 해당 기술이 기술유출 또는 부당변경에 대해 얼마나 취약한지를 나타내는 척도로서 '매우 높음(취약함)'에서부터 '매우 낮음(안전함)'까지 5가지 수준으로 구분하였는데, 판단시점에 따라 평가기준을 구분하여야 한다.

선행연구 조사/분석 단계에서는 기술유출 또는 부당변경 시도의 가능성에 중점을 두고 검토한다. 주요 작전임무의 목표 달성을 위해 무기 시스템이 어떠한 영향을 미치는지 합참 및 소요군의 협조를 받아 검토하고, 전장에서의 탈취 가능성에 대해서는 무인화 또는 원격운영 가능성, 물리적인 이동성 등을 고려하여 평가할 수 있다.

탐색개발 최종단계에서는 개념설계가 완료 또는 어느 정도 진행된 시점에서 재평가를 수행하여 그 취약성을 진단하는 데에 중점을 두어야 한다. 이미 선행연구 조사/분석 시 Anti-Tampering 기법을 적용하는 것으로 결정된 기술의 경우, 탐색개발의 수행 과정에서 개념설계를 통해 해당기술을 통해 구현될 기능이 특정 Sub-system 또는 Component에 할당되었을 것이다. 따라서 Anti-Tampering 기법 적용수준이 곧 탐색개발 최종단계에서 취약성의 척도가 될 것이다.

개조개발 검토단계에서는 무기 시스템의 실물이 이미 존재하기 때문에, 각 요소기술별로 기술유출 또는 부당변경 시도 시 성공할 가능성에 집중하는 것이 타당하다. H/W와 S/W에 대한 접근형태가 각각 다르기에 별도로 그 취약성을 평가해야 하며, 이미 Anti-Tampering이 적용된 무기 시스템의 경우에도 수출에 따른 추가 고려사항이 발생할 수 있으므로 해당내용을 최대한 반영하는 것이 적절할 것이다. 각각의 시점별로 평가척도의 세부내용을 Table 3에 간략히 제시하였다.

Table 3. Detail measurements about 'The Vulnerability'

Grade	Measurements of 1st TRA	Measurements of 2nd TRA	Measurements of Modification
Very High	· Direct impact on Operation · Unmanned or Guided weapon (Lock-On After Launched, LOAL) · Small and lightweight	· No Anti-Tampering tech. applied	· Direct access is able with commercial tools or memories
High	· Direct impact on Operation · Unmanned or Guided weapon · Small/Medium and lightweight	· Detection(with policy) or Deterrence applied · Resistance & Response not applied	· Same as above, but takes a few time or needs separation of some parts
Med	· Indirect impact on Operation · Manned or Guided weapon (Lock-On Before Launched, LOBL) · Medium and weight	· Applied Anti-Tampering tech. ≤ 2 · Response not applied	· Access is able with special tools or admin authority
Low	· Less impact on Operation · Manned or Guided weapon (only for fixed target) · Medium and weight	· Applied Anti-Tampering tech. ≤ 3	· Core tech. within sealed modular parts or admin authority within encryption module
Very Low	· No impact on Operation · Manned or Ammunition · Large and weight	· All Anti-Tampering tech. applied	· Core tech. within self-destruction parts or zeroization S/W

3.3.2 Anti-Tampering 적용여부 결정을 위한 Evaluation Matrix 도출 및 활용

'기술의 중요도' 및 '기술의 취약성'을 양 축으로 하여, Fig. 4와 같이 제시한 Evaluation Matrix를 각 요소기술별로 작성하고, Anti-Tampering 적용 필요성과 그 적용수준에 대해 판단할 수 있다.

Classification		Importance		
		High	Med	Low
Vulnerability	Very High	Red	Red	Yellow
	High	Red	Orange	Green
	Med	Orange	Yellow	Green
	Low	Yellow	Green	Green
	Very Low	Green	Green	Green

Fig. 4. Evaluation Matrix for Anti-Tampering application

Evaluation Matrix 평가 결과가 'Red'라면 '높은 수준의 Anti-Tampering 적용이 필요한 기술'로 평가된 기술이며, 'Orange', 'Yellow'의 경우 Anti-Tampering 적용 수준이 '상당' 및 '보통' 수준으로 요구되는 기술이라는 의미이다. 'Green'으로 평가될 경우, 낮은 수준으로 적용하거나 Anti-Tampering 적용이 불필요한 기술이라는 의미이다.

앞서 제시된 '기술의 취약성' 관련, 3가지 평가시점을 각각의 단계에서 평가한 결과를 사업추진기본전략 및 개발기본계획서, 탐색개발결과보고서의 부록이나 개조개발 계획에 포함시켜 Stakeholder의 의사결정을 지원할 수 있다.

한편, 특정 기술의 중요성이 부각되거나 국내외의 중대한 기술유출 사고로 인한 이슈가 발생할 경우, 언제든지 평가가 가능하도록 Evaluation Matrix의 양 축의 세부적인 평가척도를 자유롭게 변경하여 활용할 수 있다. 이때에도 혼란을 방지하기 위해 양 축의 성격은 그대로 유지되어야 할 것이다.

3.4 Anti-Tampering 기법의 분류와 수준 결정

요소기술별로 Anti-Tampering 적용 필요성을 평가하는 것만으로는 구체적인 계획을 수립할 수 없으며, 적어도 해당 요소기술을 보호하기 위해 다양한 Anti-Tampering 기법 중 어떠한 기능을 수행하는 기법을 적용할 것인지, 기능의 순서와 적용수준은 어떻게 되는지에 대한 개념을 정립하여야 한다.

Anti-Tampering 기법을 선정하는 방법론으로 위험관리의 '위험완화(Risk Mitigation)' 절차의 적용을 제시한다. '위험완화'란 '위험분석'을 통해 식별된 위험을 어떠한 방법으로 경감시킬 것인지 검토하는 것으로서 회피, 전이, 감시, 통제, 제거 등으로 구성되며[13-14], Anti-Tampering의 목적이 기술유출 위험의 완화라는 점과 억제, 감지, 방지, 반응 등의 구성분야별 성격이 위험완화 세부내용과 유사한 성격이라는 점 등을 고려하여, 논리적으로 타당하다고 판단하였다.

위험완화의 세부 내용에 대해 Anti-Tampering의 관점에서 해석한 결과, 각 보호기법들은 위험완화의 "회피, 전이, 감시, 통제, 제거"[13-14]에 대응하여 Table 4와 같이 분류할 수 있다.

Table 4. Classification of Anti-Tampering techniques (based on the concept of risk mitigation)

Anti-Tampering Techniques	Risk Mitigation
Tamper Deterrence	Risk Avoidance
Tamper Detection & Protection Policy	Risk Transfer
Protection Policy (The articles of a contract, etc.)	Risk Monitoring
Tamper Resistance	Risk Control
Tamper Response	Risk Burn-down

'위험회피(Risk Avoidance)'는 "다른 대안을 선택하여 위험이 발생할 수 있는 상황 및 조건을 감소 또는 제거하는 것"이며, 이를 Anti-Tampering의 관점에서 해석하면 "침입자가 다른 대안(즉, 침입 중단)을 취하게 함으로서 기술이 유출되는 상황이나 조건을 감소 또는 제거하는 것"이다. 따라서 '회피'는 다양한 경고문구 표시 또는 정비교범, 계약조항 등을 통해 '불필요한 접근 시도 시 법적 책임이 있음'을 경고하는 '억제(Deterrence)' 기법이다.

'위험전이(Risk Transfer)'는 "위험에 대한 책임을 제3자에게 재할당·지정하는 것"으로서, 비인가자의 침입 시도를 기록 및 저장하는 '감지(Detection)' 기법 및 각종 보호정책을 함께 적용하여 "침입/유출 시도에 따른 책임을 침입자에게 전가하는 것"이다. 여기서, 보호정책은 계약조항에 따른 주기적 확인점검을 통해 침입/유출

시도의 흔적이 발견될 시 보상 등의 책임을 묻는 것으로서, '위험감시(Risk Monitoring)'와 일맥상통한다. 한편, '감지' 기법은 침입/유출 시도의 증거를 남기기만 할 뿐이므로 반드시 보호정책이 병행되어야 한다.

'위험통제(Risk Control)'는 "위험을 수용 가능한 수준으로 낮추기 위한 활동"이며, "침입/유출 시도의 성공 가능성을 최대한 낮추고, 소요시간을 유의미한 수준으로 지연시키는 것", 즉 비인가자의 침입/유출 시도에도 불구하고 쉽게 성공할 수 없도록 하는 '방지(Resistance)' 기법으로 볼 수 있다.

'위험제거(Risk Burn-down)'는 "위험을 최종적으로 제거하는 것"으로서, "다른 보호기법에도 불구하고 계속 핵심기술에 접근할 경우, 자가파괴(H/W Self-destruction) 또는 자가삭제(S/W Zeroization)를 통해 유출대상 자체를 없애 기술유출 위험을 제거하는 것", 즉 '반응(Response)' 기법으로 볼 수 있다.

Anti-Tampering 기법은 단독으로 적용되어서는 그 목적을 달성하기 어려우며, 복합적·순차적으로 보호기능을 발휘하도록 시스템 설계에 반영해야 한다. Fig. 5는 분류별 보호기법의 Functional flow를 SysML activity diagram으로 표현한 예시이다.

한편, Anti-Tampering 기법의 기능과 순서를 각 시스템 설계에 반영함에 있어 어떤 수준으로 적용할 것인가를 판단하여야 하는데, 이는 Matrix 평가의 결과에 따라 결정하는 것이 적절할 것이다.

Chamorro는 Anti-Tamper 적용 시, 보호수준을 결정하기 위한 기준으로 미 정부의 정보처리 관련 표준인 FIPS 140-2의 활용을 제안한 바 있다[6].

FIPS 140-2는 암호화 모듈에 대한 요구사항에 관한 표준으로서, 미국 상무부 산하 국립표준기술연구소(NIST)에서 발행한다. 이는 H/W, S/W 요소를 모두 취급하며, Table 5와 같이 4단계의 보안 레벨을 제시한다[15].

Table 5. Security levels of FIPS 140-2[15]

Lv.	Details
1	The lowest, imposes very limited requirements; loosely, all components must be "production-grade" and various egregious kinds of insecurity must be absent
2	Adds requirements for physical tamper-evidence and role-based authentication
3	Adds requirements for physical tamper-resistance (making it difficult for attackers to gain access to sensitive information contained in the module) and identity-based authentication, and for a physical or logical separation between the interfaces by which "critical security parameters" enter and leave the module, and its other interfaces
4	Makes the physical security requirements more stringent, and requires robustness against environmental attacks

즉, 'Red'로 평가되면 FIPS 140-2 Lv. 3~4 수준의 기술보호를 적용하며, 'Green'으로 평가되면 Lv. 1 수준으

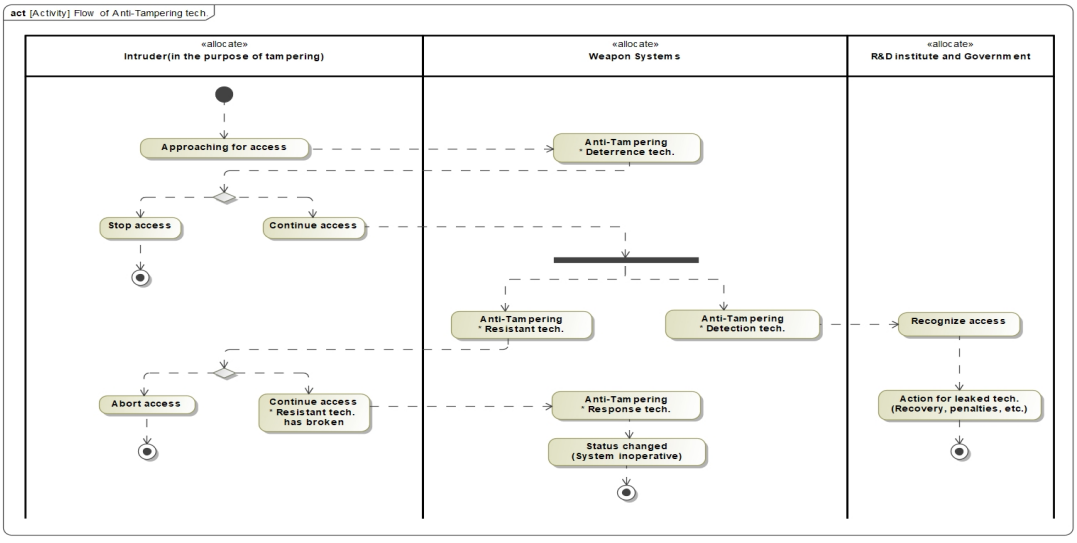


Fig. 5. SysML Activity diagram of Anti-Tampering tech.

로 갖추거나 아예 적용하지 않는 것이다. 다만, 강력한 보안수준 구현 요구사항이 추가됨에 따라 시험평가주관기관 역시 검증/확인 시 해당 표준의 인증을 요구하게 될 것이고, 이는 필연적으로 사업비용의 증가와 일정지연을 수반하기 때문에 이러한 표준을 적용하는 것은 신중한 접근이 필요하다.

4. 사례분석을 통한 유용성 확인

4.1 사례분석 대상의 개요

Table 6 및 Table 7은 본 논문에서 제안한 대로 Anti-Tampering 적용여부 판단척도인 Table 2, 3 및 Evaluation Matrix인 Fig.3에 기반하여 AA유도탄 연구개발사업 및 BB유도로켓 양산사업에 적용 및 평가결과 사례이다. 각각 '소요결정 이후 선행연구 조사/분석단계' 및 '수출소요가 발생하여 개조개발 여부를 검토하는 단계'를 가정하였으며, 이는 3.1절에서 제시한 검토시점에 부합한다.

보안상 구체적인 무기 시스템과 각 요소기술의 실제 명칭을 언급하는 것은 제한되며, 대표적으로 각각 3가지 요소기술에 대해서만 분석하였다.

4.2 사례분석 결과 요약

Table 6을 통해 AA유도탄에 적용될 기술들 중 CTE-1은 높은 수준의 기술보호가 필요한 것으로 평가되었다. 따라서 사업추진기본전략 수립 결과 획득방안이 국내연구개발로 결정되었을 경우, 개발 초기단계부터 '반응' 기법의 적용을 고려하여 설계를 수행해야 하는 것으로 추천되었다(가능할 경우, FIPS 140-2 Lv. 3~4 수준의 기술보호를 적용). 반면, CTE-2는 개발된 후 상당한 시간이 경과한 기술로서, Anti- Tampering의 적용이 불필요한 기술로 평가되었다.

CTE-3은 평이한 수준으로 보호기법을 적용하되, 탐색개발 최종단계에서 재판단이 필요한 것으로 추천되었다.

Table 7을 통해 BB유도로켓에 적용된 기술들 중 CTE-1은 반드시 보호되어야 하는 것으로 평가되었다. 따라서 수출대상국의 요구사항 반영을 위한 개조개발 시 Anti-Tampering 을 적용(가능할 경우, FIPS 140-2 Lv. 3~4 수준의 기술보호를 적용)하고, 계약조항에는 '임의 개봉 금지', '우리 기술자들에 의한 주기적 확인점검' 등의 내용을 명시하여야 한다. CTE-2 및 CTE-3의 경우는, Anti-Tampering 기법은 적용하되 낮은 수준으로도 충분하여 '억제' 기법만 적용하는 것이 추천되었다.

Table 6. Evaluation Matrix of Guided Missile's CTEs

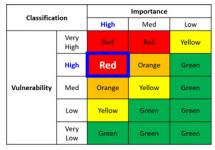
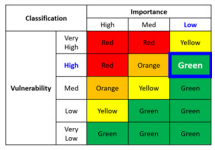
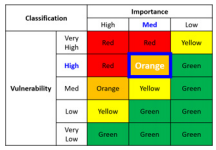
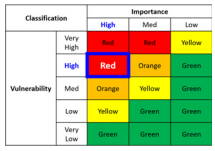
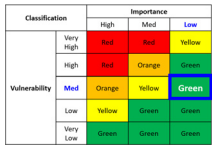
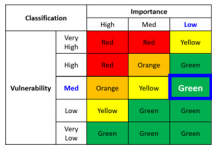
CTE	Details	Evaluation Matrix
1	• Defense industry tech.(5Y) => **High** Importance • Direct impact on Operation, Guided weapon(LOBL) => **High** Vulnerability ※ **Result : Red**	
2	• Commercial-based tech. => **Low** Importance • Direct impact on Operation, Guided weapon(LOBL) => **High** Vulnerability ※ **Result : Green**	
3	• Defense industry tech.(10Y) => **Med** Importance • Direct impact on Operation, Guided weapon(LOBL) => **High** Vulnerability ※ **Result : Orange**	

Table 7. Evaluation Matrix of Guided Rocket's CTEs

CTE	Details	Evaluation Matrix
1	• Defense industry tech.(5Y) => **High** Importance • Direct access is able with commercial tools, but needs separation of some parts => **High** Vulnerability ※ **Result : Red**	
2	• Commercial-based tech. => **Low** Importance • Access is able with special tools => **Med** Vulnerability ※ **Result : Green**	
3	• Already available in most countries => **Low** Importance • Access is able with admin authority => **Med** Vulnerability ※ **Result : Green**	

사업의 특성과 검토시점에 따라 Anti-Tampering 적용여부와 그 수준을 평가하는 것은 우리나라에 아직 정착되지 않은 분야이다. 연구를 통해 제시한 방법론은 "언제, 누가, 어떻게" Anti-Tampering 관련 검토를 수행할지에 대한 최소한의 해답이 될 것이며, 국내에서 이 분

야의 활성화에 대한 첫걸음을 내딛는 의미가 있다고 판단한다.

5. 결 론

기술수준의 발전에 따라, 국방연구개발사업 관련기관으로부터의 기술유출에 대한 대비뿐만 아니라, Tampering으로 대표되는 '무기 시스템을 통한 기술유출'에도 대비해야 한다. 또한, Tampering을 방지하기 위한 활동인 Anti-Tampering이 무기 시스템 개발비용 및 일정에 미치는 영향을 고려하여 보호대상 기술을 식별하는 절차를 마련해야 한다.

본 논문에서는 Anti-Tampering의 적용을 통해 보호해야 하는 기술을 선정하는 시점과 주관기관을 제시하였고, 위험관리 절차를 적용하여 보호대상기술의 선정과 및 다양한 Anti-Tampering 기법 중 어떤 분야의 기법을 어떤 수준으로 적용할 것인지 선정하는 방법을 제시하였다.

본 논문에서 제시한 Evaluation Matrix는 3가지 기술선정 시점(선행연구, 탐색개발, 수출시 개조개발) 이외에도 필요에 따라 언제든지 활용할 수 있으며, 중요한 기술을 보호한다는 목표를 달성하면서도 무기 시스템 개발사업의 비용 및 일정에 미치는 영향을 최소화하는데 도움을 줄 것이다.

향후 추가적인 연구과제로는, 무기 시스템 개발프로세스에 Anti-Tampering 관련활동을 통합하여 총수명주기 관점에서의 유관기관별 역할과 함께, 사업수행간 도출되는 각 산출물에 포함되어야 할 내용에 대한 연구가 필요하다.

References

[1] S. J. Ahn, C. K. Jung, K. S. Oh, J. Y. Lee, "A Study on the Development of Defence Technology Protection System," Sungkyunkwan Univ. Univ-Industry Collabo, DAPA Director General for Defense Technology Control, Oct. 2016.

[2] *Department of Defense DIRECTIVE : Anti-Tamper(AT),* DoD Directive 5200.47E, 2015.

[3] J. R. Lee, D. H. Lee, "A study on the application of the Anti-Tampering Technologies for Defense Critical Technology Protection," in Proc. 2013 KIMST General Symposium, Republic of Korea, Jeju, Jul. 4-5, 2013, pp. 78-79.

[4] H. K. Lee, W. S. Lee, Y. J. Oh, S. S. Park, "A Trend Analysis and Technology Application of Defense Technology Protection," Journal of the KIMST, Vol. 20, No. 4, pp. 579-586, 2017.
DOI : http://dx.doi.org/10.9766/KIMST.2017.20.4.579

[5] Mikhail J. Atallah, Eric D. Bryant, and Martin R. Stytz, "A survey of anti-tamper technologies," CROSSTALK : The Journal of Defense Software Engineering, vol. 17, no. 11, pp. 12-16, 2004.

[6] Alvaro Ortega Chamorro, "Physical Protection : Anti-Tamper Mechanisms in CC Security Evaluations," EPOCHE & ESPRI, Norway, 10ICCC.

[7] United States Government Accountability Office, "DoD Needs to Better support program managers' implementation of AT protection," GAO-04-302, Mar. 2004.

[8] United States Government Accountability Office, "Departmentwide Direction Is Needed for Implementation of the Anti-tamper Policy," GAO-08-91, Jan. 2008.

[9] H. J. Lee, "On the development of an Effective Defense Technology Protection System," Defense & Technology, Korea Defense Industry Association, Nov. 2017, vol. 465.

[10] *Air Force Pamphlet 63-113 : Program Protection Planning for life cycle management*, Department of the Air Force, Oct. 2013.

[11] Kristen Baldwin, Paul R Popick, John F Miller, and Jonathan Goodnight, "The United States Department of Defense revitalization of system security engineering through program protection," in Proc. Systems Conference (SysCon), 2012 IEEE International, 2012, pp. 1-7.
DOI : https://doi.org/10.1109/syscon.2012.6189463

[12] H. S. Chae, C. S. Lee, T. R. Kim, T. H. Kim, "The Design of the Response Method in Anti-tampering for UGV," in Proc. 2017 KIMST Fall Symposium, Daejeon, Republic of Korea, Nov. 14-15, 2017, pp. 819-820.

[13] *Department of Defense Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs*, Office of the Deputy Assistant Secretary of Defense for Systems Engineering, Washington, D.C. Jan. 2017.

[14] *Systems Engineering Risk Management Guidebook*, DAPA Acquisition Planning Bureau, Mar. 2018.

[15] FIPS 140, Wikipedia, Available From : https://en.wikipedia.org/wiki/FIPS_140, (accessed Sep., 2, 2018)

이 민 우(Min-Woo Lee) **[정회원]**

- 2008년 3월 : 해군사관학교 전기공학과 (공학사, 군사학사)
- 2014년 2월 : 한국외국어대학교 태국어과 (문학사)
- 2014년 2월 : 국민대학교 정치대학원 (정치학석사)
- 2015년 7월 ~ 현재 : 방위사업청 획득전문형 장교 (해군소령)
- 2016년 9월 ~ 현재 : 아주대학교 시스템공학과 (박사과정)

<관심분야>
시스템공학 (SE), Model-Based SE (MBSE), 기술보호, 요구공학 (RE), 방위력개선사업, Weapon Systems R&D

이 재 천(Jae-Chon Lee) **[정회원]**

- 1977년 2월 : 서울대학교 공과대학 전자공학과(공학사)
- 1979년 2월 / 1983년 8월 : KAIST 통신시스템 (석/박사)
- 1984년 9월 ~ 1985년 9월 : 미국 MIT Post Doc 연구원
- 1985년 10월 ~ 1986년 10월 : 미국 Univ. of California 방문연구원
- 1990년 2월 ~ 1991년 2월 : 캐나다 Univ. of Victoria (Victoria, BC) 방문교수
- 2002년 3월 ~ 2003년 2월 : 미국 Stanford Univ. 방문교수
- 1994년 9월 ~ 현재 : 아주대학교 시스템공학과 정교수

<관심분야>
시스템공학 (SE), Model-Based SE (MBSE), Systems Safety, System T&E, Modeling & Simulation