https://doi.org/10.33778/kcsa.2019.19.4.067

무기체계 수명주기 간 사이버보안 적용 개선방안

정 용 태*, 정 현 식**, 강 지 원***

요 약

최근 국방부는 무기체계를 사이버보안의 영역에서 무기체계를 포함하였다. 기존 정보화영역에 한정되었던 사이버보안의 대상에서 확대되고 진화된 개념이 적용되었다. 무기체계는 소프트웨어의 비중이 점차 늘어나고 있고, 사이버위협의 대상임에는 분명하다. 따라서, 사이버보안 측면에서 무기체계 수명주기간 문제점을 진단하여 무기체계 사이버보안 발전방향을 제시하고자 한다. 무기체계 사이버보안 발전을 위해서는 무기체계 소프트웨어 관리제도를 포함하여 종합적인 정책수립이 이루어져야 하고, 이와 관련된 이해관계자들의 적극적인 참여가 필요하다.

A Study on Enhancing Cybersecurity of Weapon Systems for Life-Cycle

Yong-Tae Jung*, Hyun-Sik Jung**, Ji-Won Kang***

ABSTRACT

Recently, the Ministry of National Defense has included embedded software for weapon systems as targets for the Defense cyber security. The Concept has been extended and evolved from the cyber security area that was previously limited to the information domain. The software is becoming increasingly important in weapon systems, and it is clear that they are subject to cyber threats. Therefore, We would like to suggest a improvement direction by diagnosing problems in terms of cyber security of the weapon systems for the life cycle. In order to improve cyber security of weapon systems, comprehensive policy including the weapon embedded software management should be established and the involved stakeholder should be participated in the activities.

Key words : Cyber security, Weapon systems, Embedded software, Vulnerability

접수일(2019년 10월 4일), 게재확정일(2019년 10월 28일)

* 국방부
** 숭실대학교 IT정책경영학과
*** 세종대학교 컴퓨터공학과(교신저자)

1. 서 론

지난해 12월 국방부 훈령인 '국방사이버안보 훈령'이 대폭 개정되었다. 특히 눈에 띄는 내용은 국방 내 사이버안보의 대상을 "정확하고 안전하며 효과적인 국방 사이버공간의 창출·유지·보호를 위하여 국방정보시스템과 내장형 소프트웨어(Embedded Software)를 가지고 있는 무기체계 및 전력지원체계"라고 규정한 부분이다. 이는 기존에 국방 사이버보안 업무영역을 국방정보시스템으로 한정하여 무기체계로 분류되는 정보시스템[1]과 정보화사업으로 소요제기하는 전력지원체계에 적용하였던 것에 비해 엄청난 영역의 확대와 개념의 진화라고 볼 수 있다. 또한 사이버보안 업무를 "국방 사이버공간에서 정보의 기밀성·무결성·가용성을 보장하기 위하여 취하는 물리적, 기술적, 관리적 활동"으로 정의하고, 국방정보시스템과 내장형 소프트웨어(Embedded Software)를 가지고 있는 무기체계 및 전력지원체계의 수명주기와 연계한 보안활동으로 그 업무를 명시하고 있다[1].

예측하기 힘든 다양한 사이버 위협이 현실화되고 있는 시점에서 국방 사이버보안의 영역과 대상을 내장형 소프트웨어를 가지고 있는 무기체계 및 전력지원체계까지 확장되는 것은 바람직한 일이다. 하지만 이러한 업무 영역의 확장은 시스템의 수명주기간 실행되어야 하는 보호 업무들을 수행하여야 할 관계기관·부서의 합의가 이루어지지 않으면 실현이 불가능할 것이다. 이를 실현하기 위해서는 국방 사이버공간을 생성하고, 이용하며 유지하는 모든 이해관계자들의 합의가 반드시 선행되어야 하고 각자의 주어진 임무를 수행하여야만 가능한 일이라 할 수 있다.

한편, 무기체계는 고도화됨에 따라 요구기능을 소프트웨어로 구현하는 비율이 점차 높아지고 있다[2]. 미국의 경우, 과거 F-4 전투기는 전체 기능 중 소프트웨어로 구현된 비율이 8%에 불과하였으나 F-35는 90%에 이르고[3], 한국해군 구축함의 경우, 1990년대 광개토대왕함급 전투체계의 소스코드는 1만 라인이 되지 않았으나, 2010년대 세종대왕함급 이지스전투체계의 소스코드는 7만 라인에 이르는 것으로 알려져 있다. 이러한 무기체계 기능구현의 기술적 변화는 무기체계 소프트웨어 비중의 확대를 가져왔으나, 이는 곧 무기체계가 보안성 결함에 의해 사이버위협에 더 많이 노출될 수 있음을 의미한다. 최근 언론은 무기체계 소프트웨어의 보안성 결함을 이용한 사이버위협에 대해 크게 우려하고 있다[4, 5].

본 연구에서는 사이버보안의 개념이 변화된 과정을 통해 현재 풀어야할 과제를 살펴보고, 국방사이버보안의 대상으로 확대된 무기체계 소프트웨어의 특성을 이해한 다음, 사이버보안 측면에서 무기체계 수명주기간 소프트웨어 관리실태를 진단하여 발전방안을 제시하고자 한다.

2. 무기체계 사이버보안 관련 연구

2.1 정보보호에서 사이버보안으로 개념 진화

현재 국방 사이버보안의 시작은 2001년으로 거슬러 올라간다. 국방부는 '정보시스템과 정보자료 보호'를 목적으로 국방정보통신망을 보호하기 위해, CERT(Computer Emergency Response Team)를 편성하고, 통합보안관제체계를 도입하여 국방사이버상황실을 개설하는 등 군사정보자료 유출방지를 위한 제도, 조직, 체계를 구축하였다. 당시 국내에는 정보화와 더불어 정보보호의 중요성을 고려하여 정보통신기반보호법(2001.7월), 공공기관의 정보보호 및 개인정보보호에 관한 법률(1995.1월)[2] , 전자정부구현을위한행정업무등의전자화촉진에관한법률(2001.7월)[3] 등 공공기관 정보보호에 대한 관심이 집중되던 시기였다. 국방부에서도 이를 이행하기 위해 2002년 4월 국방정보보호훈령을 제정하여 시행하고, 2008년 3월에는 정보보호 전담조직으로 정보화기획관실 내에 8명으로 편성된 정보보호팀을 신설하였다.

이후, 국방부는 2011. 1월 국방정보화법을 제정하여 시행하고, 국방정보보호 훈령을 포함한 흩어져있는 정보화 관련 훈령들을 통합하여 2011.2월 국방정보화업

1) 국방전력발전업무 훈령의 무기체계 분류에 따르면 지휘통제체계로 분류되는 전장관리체계와 M&S체계로 분류되는 워게임모델 등이 이에 해당한다.

2) 2011.3월, 개인정보보호법 제정으로 폐지

3) 2007.1월, 전자정부법으로 변경 시행

무훈령을 제정하여 시행하면서 기존의 '국방정보보호 훈령'의 내용은 국방정보화업무훈령에 통합 수록하였다. 정보보호업무는 조직과 제도적으로 정보화의 영역에서 통합 수행하는 환경이 완성되었다.

또한, 2004년 2월, 국정원은 사이버테러로부터 국가정보통신망을 보호하려는 목적으로 사이버테러 감시, 예방, 경고 등의 임무를 수행하기 위해 국가사이버안전센터를 설립하고, 이에 대한 법적근거로 2005년 1월 국가사이버 안전관리규정을 시행하였다. 정부 차원에서 공식적으로 처음 '사이버'라는 용어가 등장하였다.

국방부는 2008년 국가안보위협의 대상으로 "사이버 공격"을 처음으로 포함하였다[6]. 2010년 1월에는 국방정보시스템에 대한 사이버 위협을 대응하기 위해 국군사이버사령부를 창설하였고, 2012년 3월에는 국방부의 기존 정보보호팀을 사이버방호정책팀으로 확대 개편하였다. 2013년 3월에는 사이버방호정책팀을 사이버방호정책과로 확대 개편 하였고, 2017년 2월에는 2016년 국방망 해킹사고 후속조치 업무와 연계하여 인원을 대폭 증원한 사이버정책과로 확대 개편하였다. 2017년 5월에는 사이버정책과에서 위기대응과 체계기술 업무를 분리하여 사이버대응기술팀을 조직하였다. 국방정보시스템의 다양화와 고도화로 지속적으로 업무가 확대되었으며 이에 맞추어 조직 또한 확대 개편되었다. 또한, 국방부 훈령은 2014년 7월 국방정보화업무훈령에서 정보보호 관리분야를 별도로 분리하여 사이버작전을 포함한 국방사이버안보훈령으로 제정하였다.

공식적인 용어가 '정보보호'에서 '사이버보안'으로 변화하고 있지만, 사이버영역은 네트워크가 연결된 국방정보시스템의 영역 내에서 이루어졌다. 다시 말해, 사이버보안업무는 무기체계 내 일부 정보시스템과 정보화사업으로 소요제기되는 전력지원체계를 대상으로, 정보시스템을 획득하고 관리하고 운용하는 정보화업무수행 조직(정보통신병과)들 간에 이루어졌다.

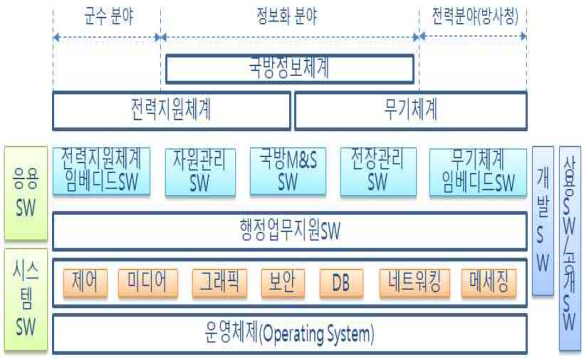
지금까지 살펴 본 정보보호에서 사이버보안까지의 개념적인 진화 과정을 종합하면, 2001년부터 현재까지, 국방정보화의 가속화를 통해 업무환경은 편리하게 되었지만, 국방정보통신망과 국방정보시스템의 복잡 다양화로 인하여 보호해야 할 대상들이 대폭 확대되었다. 사이버공간을 정보화 영역인 국방정보통신망과 국방정보시스템으로 한정한다면 정보화 조직으로만 사이버보안을 수행할 수 있겠지만, 사이버공간을 정보기술(Information Technology)이 적용된 모든 무기체계와 전력지원체계로 확대하기 위해서는 모든 국방영역에서 관련 조직이 함께 다루어야 한다. 사이버공간을 생성하고 이용하고 관리하는 모든 관계자가 이해당사자로서 사이버보안 활동을 주체적으로 수행하여야 한다. 예를 들어 무기체계의 경우, 소요기획, 획득, 전력화, 운용유지, 폐기 등 전 수명주기에 관여하는 조직과 기관이 이에 해당한다고 할 수 있다.

2.2 무기체계 소프트웨어 구분과 관리

(그림 1) 국방 소프트웨어의 구분

국방분야에서 소프트웨어는 (그림 1)과 같이 체계, 계층 및 영역의 3가지 기준으로 구분할 수 있는데, 체계기준으로 무기체계와 전력지원체계로 구분하고, 계층기준으로 임무응용소프트웨어와 시스템소프트웨어로 구분하며, 영역기준으로는 정보화영역과 비정보화영역으로 구분할 수 있다.

무기체계 소프트웨어는 "유도무기・항공기・함정 등 전장(戰場)에서 전투력을 발휘하기 위한 무기와 이의 운영에 필요한 제반요소를 통합한 무기체계에 포함된 소프트웨어"로 정의할 수 있는데, 국방 소프트웨어의 구분에서는 무기체계로 분류된 비정보화 영역의 임무응용소프트웨어와 시스템소프트웨어가 이에 해당한다고 할 수 있다.



(그림 2) 국방 소프트웨어 구조

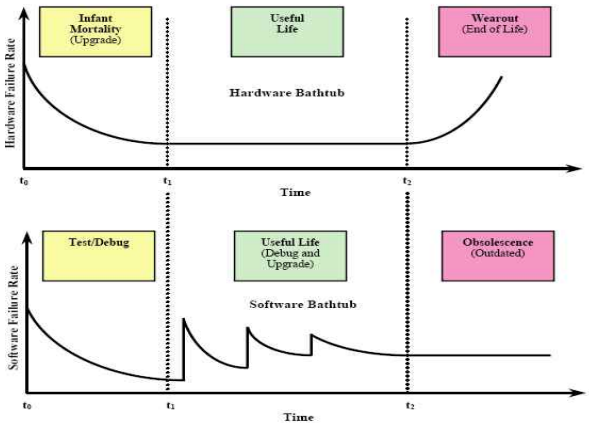
앞서 설명하는 무기체계 소프트웨어 구분을 조금 더 구체화 하면 (그림 2)와 같이 무기체계 소프트웨어의 구조를 정리할 수 있다. 정보화 영역과 비정보화 영역(군수, 전력)으로 구분하고, 소프트웨어 계층을 시스템 소프트웨어와 응용 소프트웨어로 구분하여 2차원 모형으로 정리가 가능하다. 국방정보시스템은 정보화 예산으로 획득하는 순수 정보시스템과 전력지원체계와 무기체계 중 소프트웨어 개발 비중이 높은 정보시스템(예 : C4I시스템 등)을 포함하여 사이버보안이라는 우산을 씌우고 있다.

일반적으로 국방 무기체계 소프트웨어는 일반 소프트웨어와 는 다른 특징을 가지고 있다. 첫째, 무기체계의 원래의 성능을 발휘하여 주어진 임무를 일정 시간 내 정확히 수행되어야 하는 실시간 운영체제라는 것이다. 둘째, 불완전한 상황 및 전자 환경 속에서도 거의 완벽한 운영 가용성을 유지하여야 한다. 셋째, 시간, 장소 및 기타 환경과 무관한 완결성 있는 무기체계로 작동을 하여야 하는 고신뢰성을 보장하는 것이다. 넷째, 무기체계 간 데이터 및 시스템 간의 연동되어 원활한 운영이 가능하도록 상호운용성을 확보하는 것이다. 마지막으로 하드웨어와 동시 개발되는 경우가 많기 때문에 시스템 형상변경 및 요구사항 수정 등에 대해 지속적으로 개발개념 변화와 적응에 따른 노력이 필요하다.

정보기술의 발달은 무기체계에 적용되는 소프트웨어의 규모의 증가를 가져왔고, 하드웨어 보다 소프트웨어에서 더 많은 기능통제 역할을 담당하게 되었다. 따라서 무기체계의 하드웨어 고장정비 뿐만 아니라 소프트웨어 운용유지는 더 중요한 부분이 되었다.

무기체계는 운용유지 측면에서 크게 하드웨어와 소프트웨어로 나누어 이해할 수 있는데, 무기체계 수명주기 관점에서 보면 (그림 3)와 같이 나타낼 수 있다.

하드웨어는 전력화 이전 안정화되기까지 고장률이 점차 낮아지다가 운용단계에는 안정세를 나타내고 수명주기 마지막 단계에는 노후로 인한 고장률이 급격하게 상승한다. 반면 소프트웨어는 전력화 이전 테스트를 통해 결함을 찾아내어 수정 보완하면서 결함도가 점차 낮아지다가 운용단계에서 찾아낸 소프트웨어 결함에 대한 개선 및 패치 등으로 짧은 주기로 고장과 안정화를 반복하게 된다. 이러한 과정을 거치면 마지막 단계에는 안정적으로 운용하게 된다[7].



(그림 3) 수명주기 간 HW와 SW 고장률

무기체계의 수명주기 동안에 하드웨어와 소프트웨어의 고장이 발생하게 된다. 하드웨어는 물리적인 노화나 사용자의 실수가 고장의 원인인 반면에 소프트웨어는 설계-구현-시험단계에서 결함이 생성되기도 하고 식별되어 수정되기도 한다. 이 단계에서 식별되지 않은 결함은 운용단계에서 고장의 원인이 된다. 소프트웨어의 결함은 최초 개발시 식별되지 않고 잠재되어 있거나, 전력화 이후 결함의 개선을 위한 수정과 기능의 추가를 위한 성능개선 등의 소프트웨어 변경 시에도 예상하지 못한 과정에서 새로운 결함이 추가될 가능성이 있다. 소프트웨어 결함은 많은 시험을 통해서 결함을 줄일 수 있지만 완전하게 결함이 제거되었는지 측정하는 것은 제한된다. 사이버위협 측면에서, 사이버 공격의 약 75%가 소프트웨어의 보안성 결함인 취약점을 이용한 악의적인 공격에 기인하기 때문에 무기체계

의 소프트웨어 보안성은 대단히 중요하다[8].

무기체계에 고장이 발생하면, 하드웨어는 원상태로 복구하기 위하여 부품교환 또는 수리형태로 정비가 이루어지는 반면, 소프트웨어는 개발과정에서 생성된 결함을 제거하기 위해서 소프트웨어 변경이라는 형태로 정비가 이루어진다. 고장예방을 위한 조치로, 하드웨어는 청소, 조임, 손질, 조정 등으로 예방정비를 실시하지만, 소프트웨어는 오류검사를 통하여 잠재된 결함을 찾아내는 예방정비를 실시하여야 한다[9].

<표 1>에서 무기체계의 하드웨어와 소프트웨어의 고장과 정비 특징을 비교하였다.

<표 1> HW와 SW 고장-정비 특징 비교

구 분	하드웨어	소프트웨어
고 장	고장징후 감지 가능	사전경고 없음
고장원인	개발, 생산, 운용 전분야	개발상 오류
정 비	원상태로 복구	SW 수정
정비방법	청소, 조임, 조정, 교환	SW 변경, 삭제, 조정
시 험	소모적 시험 가능 물리적 측정 가능	무한시험 물리적 측정 불가

소프트웨어 변경이 필요한 대부분의 정비업무는 별도의 개발로 간주하여 개발업체의 외주정비를 통해서만 이루어질 수 있다. 따라서 무기체계 수명주기 동안 지속적으로 소프트웨어 보안성을 보장하기 위해서는 무기체계 정비계획에 포함하여 결함(취약점)을 정기적으로 점검하고 식별된 결함을 제거하기 위해 소프트웨어를 즉시 변경하도록 체계화하여야 한다.

2.3 무기체계 소프트웨어 관리 수명주기

(그림 4) 국방 무기체계 소프트웨어 수명주기

(그림 4)와 같이 국방무기체계 소프트웨어 수명주기에서 첫 단계는 무기체계 소요기획 단계이다. 국방기본정책서, 군사전략서를 바탕으로 합참이 합동개념을 발전시키고 이를 구체화(세부 개념화) 하고 미래작전능력 요구를 기준으로 개념소요를 도출한다. 또한, 각 군이 전투실험과 사전분석을 통해 소요제안을 구체화 하여 소요제기서를 작성하여 합참으로 제기하며, 합참은 합동성 차원에서 검토·조정하여 전력소요서(안)을 만들며 심의·의결을 통해 소요를 결정한다.

소요결정 이후 예산단계로, 국방부에서 중기계획 수립 지침을 하달하고 각 군 및 기관이 전력운영분야 사업계획과 방위력개선분야 전력화지원소요를 작성하여 각각 국방부와 방위사업청으로 제출하며 이를 검토·조정한 후 국방부에서 최종 심의·의결하고 대통령 승인을 받아 확정한다. 또한, 국방부 예산편성지침에 따라 각군 및 기관이 사업별 예산요구서를 작성하여 국방부와 방사청 검토·조정을 거쳐 장관 보고하고 이를 종합하여 기재부로 제출하며 기재부 검토가 완료되면 국회 예산심의를 받아 최종 예산을 편성한다.

방위사업청에서는 비용대 효과 및 국가이익을 함께 고려하여 자체적으로 연구개발하거나 구매를 판단하고 결정된 사업의 집행을 통해 획득한다.

이어서 소프트웨어 개발과정의 마지막 단계인 개발/운영 시험평가와 규격화를 거치면 무기체계와 전력지원체계는 소요군인 각 군의 군수 조직에 인수인계 되고 전력화를 추진하며 대부분의 경우 하드웨어 정비를

주 업무로 하는 조직이 소프트웨어를 포함하여 동시에 유지보수를 담당한다.

3. 무기체계 사이버보안 관리 실태

국방 소프트웨어 분류에 따르면 무기체계 소프트웨어는 정보화의 영역을 벗어나 있기 때문에, 국방부 내 소관하는 부서가 다르고 정보화 영역의 소프트웨어와 다르게 관리되고 있다. 또한 무기체계 소프트웨어의 수명주기 측면에서 보면, 전력화 이전과 이후로 소관하는 기관이 다르고 전력화 이후에는 지속적인 관리가 어려운 실정이다. 이에 현행 무기체계 소프트웨어 보안관리 실태를 진단해 보면 다음의 4가지로 요약할 수 있다.

3.1 무기체계 소프트웨어 관리 주체

현재 무기체계 소프트웨어 업무를 주관하는 부서가 모호한 상황이다. 방위사업청(이하 '방사청') 개청 이전에는 국방부 연구개발관실이 무기체계 소프트웨어 정책에 대해 컨트롤타워 역할을 수행하고, 기존의 국방획득관리규정에 명시된 부서 및 기관의 업무와 유사하게 정립하여 '무기/비무기체계 내장형 소프트웨어 개발관리 지침(2002. 1월)'을 시행하였다. 2006년, 무기체계 획득업무가 방위사업청으로 이관되면서, 방위사업청은 획득정책/제도 위주로 무기체계 소프트웨어 발전전략을 추진하였다. 이에 무기체계 수명주기 전 기간에 걸친 종합적인 무기체계 소프트웨어 관리정책/제도가 정착되지 못하고 전력화 전·후를 구분하여 컨트롤타워가 모호하게 되었다. 더욱이 무기체계 전 수명주기에 걸쳐 검증되고 관리되어야 할 무기체계 소프트웨어의 보안업무는 고려되지 못하였다.

3.2 무기체계 소프트웨어 보안성 유지

무기체계 소요기획, 획득, 운용유지 간 이해관계자들이 무기체계 소프트웨어 보안성에 대한 관심이 부족한 실정이다. 국방부에서 "무기/비무기체계 내장형 소프트웨어 개발관리 지침"을 제정한 이후, 방위사업청은 무기체계 소프트웨어의 신뢰성과 품질을 위해 지속적으로 노력하여 왔다. 이러한 무기체계 획득시 소프트웨어의 신뢰성과 품질 중심의 획득 추진전략으로 인하여 무기체계 소프트웨어 보안성에 대한 관심은 상대적으로 소홀한 측면이 있었다. 무기체계의 소요기획, 획득, 운용유지 등 수명주기 전 기간에 이해관계자라 할 수 있는 국방부(전력정책, 군수관리, 정보화), 방위사업청 및 소요군 간 무기체계 소프트웨어에 대한 일관성 있는 보안성 관리정책이 미흡하다.

3.3 무기체계 소프트웨어 보안성 시험·검증

무기체계 소프트웨어 보안성에 대한 현재의 시험 및 검증제도는 한계가 있다. 방위사업청은 무기체계 소프트웨어의 품질을 확보하기 위한 목적으로 소프트웨어 신뢰성 시험과 소프트웨어 보안성 시험을 시행하고 있다. 이는 제도가 정립된 2011년 이후부터 전력화하는 무기체계에 적용하고 있으며, 소프트웨어 보안성 시험은 전장관리정보체계(정보시스템)에 한정하여 실시하고 있다. 또한 개발시험 이후 변경된 소프트웨어에 대해서는 연구개발주관기관이 자체시험을 실시하고 결과만 확인하는 절차로 진행하여 실질적인 검증이 제한된다. 또한 '국방정보보안시스템 업무훈령'에 따르면 무기체계 소프트웨어에 대해 안정성 검증을 시행토록 하고 있지만 보안시스템이 설치된 국방정보통신망과 비밀이 소통되는 무기체계 소프트웨어로 한정하고 있고 각급부대의 장이 안전성 검증을 신청하는 절차로 되어 있어, 신청 사례가 거의 없는 것으로 알려져 있다.

3.4 전력화 이후 무기체계 소프트웨어 관리

무기체계 전력화 이후의 소프트웨어 관리업무는 소요군으로 이관되어 체계적인 관리가 미흡한 부분이 있다. 무기체계는 획득시 정비개념을 정립하고 전력화 이후 무기체계 운용단계에 각 군에서 정비업무를 수행하고 있지만, 하드웨어 위주의 종합군수지원(ILS : Integrated Logistics Support) 요소 개발에 따른 정비계획으로 소프트웨어에 대한 예방정비 등 정비개념이 미흡한 실정이다. 특히, 잠재적으로 내재된 소프트웨어 보안성 결함(취약점)에 대해서는 운용단계에 정기·수시로 점검하고 정비하는 개념은 전혀 없다. 현재는 소

프트웨어 결함 확인 시에 품질보증 절차에 따라 하자 보증 처리를 통하여 보완하고 있지만, 전력화 이후 변경된 소프트웨어에 대해서는 별도의 보안성 재검증 절차가 없어 신규 추가된 소프트웨어 보안성 결함(취약점)에 대한 확인은 불가능 한 것이다.

무기체계 소프트웨어의 보안성은 소요기획, 획득, 운용유지 등 수명주기 전 기간에 걸쳐 관리될 수 있어야 한다. 이를 위해서는 무기체계 획득 및 운용유지 관계기관 및 부서의 인식전환이 필요하고, 무기체계 전력화 이후 소프트웨어의 보안성에 대해 점검하고 정비할 수 있는 종합군수지원계획을 수립하여 지속적으로 소프트웨어 보안성 검증이 이루어 질 수 있도록 제도적인 발전이 요구된다.

4. 무기체계 사이버보안 적용 개선방안

무기체계 수명주기 간 사이버보안 발전방향을 제시하기 위하여 (그림 5)와 같이 3가지 추진전략과 이에 대한 핵심과제를 도출하였다. 관련 내용으로 보완되어야 할 적용규정은 국방전력발전업무훈령, 국방사이버안보훈령, 국방보안업무훈령, 방위사업관리규정 등이 있다.

(그림 5) 무기체계 수명주기간 사이버보안 발전방향(안)

4.1 무기체계 소프트웨어 보안성 제도 개선

무기체계 소프트웨어 보안성에 관련된 제도를 개선하여야 하겠다. 무기체계 획득 및 운용과 관련하여 소프트웨어 보안성 강화를 위한 정책과 제도를 개선 추진하기 위해서는 무기체계 소프트웨어에 대한 임무 정립을 선행하여야 한다. 무기체계 소프트웨어를 무기체계와 별개로 볼 것이 아니라, 무기체계 소요, 획득 및 운용단계에서 소프트웨어 보안성이 연계될 수 있도록 기관 및 부대별로 임무를 명확히 할 필요가 있다. 무기체계의 전력증강 정책을 수립하는 전력정책관실, 무기체계의 획득정책을 수립하는 방위사업청, 무기체계의 군수지원정책을 수립하는 군수관리관실 및 무기체계 소프트웨어 보안기술 정책을 지원하는 정보화기획관실 등이 대표적인 기관/부서라고 할 수 있다.

대표적인 기관/부서는 정책적인 제도를 통하여 무기체계 소프트웨어 관련 업무를 통제하고 각 군 및 기관이 수행할 수 있는 여건을 마련하여야 한다. 이를 요약하면 <표 2>와 같이 정리할 수 있다.

<표 2> 무기체계 소프트웨어 보안성 정책 임무 정립(안)

구 분	정책기관	수행기관
수명주기 전력증강정책	국방부(전력)	합참(전력), 각군(전력)
운용단계 취약점 조치	국방부(군수)	각군(군수), 군수사
보안성 검증	국방부(정보화)	사이버작전사, 군사안보지원사
획득단계 취약점 제거	방위사업청	방산기술지원센터, 기품원

4.2 무기체계 소프트웨어 보안성 검증 강화

무기체계 소프트웨어에 대한 보안성 검증을 강화하여야 하겠다. 첫째, 현행 연구개발시 수행 중인 보안대책 검토 및 보안측정 등을 정비하여 종합적인 보안성 검증절차로 정립할 필요가 있다. 현재, 군사안보지원사는 소요단계부터 보안대책을 검토하고 개발단계에는 보안요구사항, 보안설계사항 검토 및 소프트웨어 보안성 진단을 수행하고 있으며, 사이버작전사는 자체적으로 운용단계에서 무기체계 취약점 점검을 수행하기 위한 능력을 배양하고 있다. 방위사업청은 2011년부터 무기체계에 대한 소프트웨어 신뢰성 시험을 도입하여 체계개발 과정에서 시행하고 있고, 국방기술품질원에서도 SW의 품질관리 측면에서 무기체계의 SW를 관

리하고 있다. 둘째, 무기체계 전력화 이후 운용단계에서 변경된 무기체계 소프트웨어에 대한 보안성 재검증을 실시하여야 한다. 무기체계는 전력화 이후에도 오류수정, 기능개선 등의 사유로 소프트웨어의 형상을 변경하고 관리하고 있으나, 이 과정에서 변경된 무기체계 소프트웨어에 대한 보안성 검증은 제대로 이루어지지 않고 있는 실정이다. 무기체계 전력화 이후에도 지속적으로 하자보증 또는 정비계획, 형상관리, 보안성 검증이 연계될 수 있도록 종합군수지원계획으로 발전시켜 관리되어야 할 것이다.

마지막으로 상시 무기체계 소프트웨어에 대한 보안성 진단체계를 구축하여야 한다. 사이버 위협의 공격기술과 방어기술은 병행적으로 발전하고 있다. 체계개발 및 전력화 단계까지 식별되지 않은 잠재적인 보안성 결함은 전력화 초기에는 식별이 되지 않지만 취약점 식별도구의 발전과 점검요원의 숙련도에 따라 운용중에도 새롭게 식별될 수 있다. 지능형 지속공격(APT)의 관점에서도 위협은 특정한 여건이 성숙될 때까지 운용단계에서 잠재적으로만 존재하도록 설계할 수 있다. 운용단계에서 모의침투 또는 취약점 점검을 통해 지속적으로 확인할 수 있도록 상시 보안성 진단 제도를 마련하여야 하겠다.

4.3 무기체계 소프트웨어 보안성 관리체계 구축

무기체계 소프트웨어 보안성을 관리할 수 있도록 체계를 구축하여야 하겠다. 첫째, 무기체계 수명주기 전 기간에 소프트웨어 보안성 관리가 이루어지기 위해서는 종합군수지원계획에 따른 소프트웨어 점검과 정비가 체계적으로 이루어져야 한다. 무기체계와 함께 종합군수지원요소도 개발하게 되는데, 무기체계 소프트웨어 정비계획을 개발하여야 한다.

예를 들어, 무기체계 운용 간에 예방정비 차원에서 소프트웨어 보안성 점검을 시행하고 식별된 보안성 결함에 대해서는 정비계획에 따라 자연스럽게 소프트웨어 정비가 이루지는 것이다. 둘째, 무기체계 소프트웨어 보안성 관리 전담기관을 지정이 필요하다. 무기체계 전력화 전·후로 나뉘어 군사안보지원사와 사이버작전사로 이원화 되어 무기체계 소프트웨어 보안성 업무를 수행하고 있다. 효율적인 무기체계 소프트웨어 보안성 관리를 위해서는 2개 기관이 합동으로 업무를 수행하거나 통합하여 전담기관을 지정할 필요가 있다.

마지막으로 무기체계 소프트웨어 보안성 관리지침을 명문화할 필요가 있다. 무기체계 수명주기 전 기간에 단계별로 소프트웨어 보안성 관리가 이루어 질 수 있도록 관계기관별 책임과 권한을 명확히 하여야 하겠다.

5. 결 론

적의 사이버위협으로부터 무기체계를 안전하게 보호하기 위해서는 무기체계 소프트웨어 보안성 확보가 반드시 필요하다. 무기체계의 영역에서는 현재와 같은 형태로 정보화 영역 내에서 정보화 조직으로만 수행하기에는 한계가 있다. 사이버보안 측면에서 현행 무기체계 소프트웨어 관련 정책・제도・절차적 문제점을 해결하기 위해 3대 추진전략을 발전방향으로 제시하였다. 이를 통해 신규 무기체계의 경우, 소요단계부터 운용단계까지 무기체계 소프트웨어 보안성의 안정적 관리가 가능할 것으로 예상한다. 추가적으로 무기체계 소프트웨어 관리제도 개선과 무기체계 소프트웨어 종합군수지원 개념 정립에도 긍정적 영향을 미칠 것으로 기대한다. 이를 위해서는 무기체계 소프트웨어 관리제도를 포함하여 종합적인 정책수립이 이루어져야 하고, 모든 이해관계자들의 주체적인 사이버보안 활동이 요구된다.

참고문헌

[1] 국방부, ‘국방사이버안보 훈령’, 제2234호, 2018.
[2] Mark H. Ralston, ‘Software Evaluation: Toward a Rigorous Approach’, U.S. AMSAA, 1996.
[3] Firesmith, Donald G., et al. ‘The method framework for engineering system architectures’, Aurebach Publications, 2008.
[4] 이정규, ’무기체계 사이버 보안 정책 동향‘, 정보보호학회지, 제28권, 제6호, pp.83-87, 2018.
[5] 전자신문, ‘무기체계 SW 보안성 검증했더니... 기본도 안지켰다’, 2018.6.19.일자

[6] 국방부, '2008년 국방백서', 2008.
[7] 이관영 외, '소프트웨어 ILS 적용방안 연구: 소프트웨어와 하드웨어 유지보수 특성을 고려한 비교분석을 중심으로', 한국산학기술학회지, 제15권, 제9호, pp.5726-5737, 2014.
[8] Symantec, 'Internet Security Threat Report', 2011 Trends, Vol. 17, April 2012.
[9] 심행근 외, '소프트웨어에 대한 종합군수지원(ILS) 적용방안', 한국군사과학기술학회지, 제2권, 제2호, pp.173-185, 1999.

〔저자소개〕

정 용 태 (Yong-Tae Jung)
1997년 2월 해군사관학교 학사
2005년 2월 포항공과대학교 석사
2019년 8월 한남대학교 산업공학 박사
2018년 1월~현재 국방부
email : yt.jung@gmail.com

정 현 식 (Hyun-Sick Jung)
1992년 3월 해군사관학교 전기공학 학사
2006년 6월 동국대학교 사회과학대학원 (경영정보) 석사
2019년 3월~현재 숭실대학교 IT 정책경영학 박사과정
email : mnd5918@mnd.go.kr

강 지 원 (Ji-Won Kang)
1988년 2월 금오공대 전자공학 학사
1997년 2월 연세대학교 컴퓨터과학 (정보보호 전공) 석사
2012년 8월 경기대학교 정보보호학 박사
2017년 9월~현재 세종대학교 컴퓨터 공학과 산학협력중점교수
email : jwkang@sejong.ac.kr