한국방위산업학회
제19권 제2호
2012년 12월

사이버전 대응을 위한 국방 SW 개발보안 적용 방안
- 무기체계 내장형 SW 적용 수준을 중심으로 -

최준성[1] 김우제[2] 박원형[3] 국광호[4†]

내용목차

1 주저자, 서울과학기술대학교 IT정책전문대학원 산업정보시스템전공 박사과정
2 서울과학기술대학교 기술경영융합대학 글로벌융합산업공학과 교수
3 극동대학교 사이버안보학과 교수
4† 교신저자, 서울과학기술대학교 기술경영융합대학 글로벌융합산업공학과 교수
(Tel: 031-8020-7026, E-mail: where@seoultech.ac.kr)
※ 본 연구는 2012 한국경영과학회추계학술대회/방위사업청 무기체계시험평가세미나 "무기체계내장형 SW 개발보안 적용방안"발표를 확장한 것임.

논문접수일: 2012년 12월 14일 게재확정일: 2012년 12월 24일
논문수정일: (1차: 2012년 12월 17일 2차: 2012년 12월 20일)

Korea Association of
Defense Industry Studies
Vol.19, No.2, December 2012

Defense SW Secure Coding Application Method for Cyberwarfare Focused on the Warfare System Embedded SW Application Level

Choi, June Sung[1] Kim, Woo Je[2] Park, Won Hyung[3]
Kook, Kwang Ho[4†]

Abstract

The need for security in the SDLC (SW Development Life Cycle) has been increasing. Also, it is well-known that the error correction cost in the SW operational phase is soaring highly compared with that in the design phase. On the other hand, it is known that the security vulnerabilities have decreased with the application of Secure Coding in the design phase. Security for the warfare systems embedded SW of defense SW is very important, though, but has not yet been discussed. In this paper, defense SW factors and methods, especially the warfare systems embedded SW, are discussed.

<Keywords> Secure Coding, Defense Software, Warfare System Embedded Software

1. 연구 배경

최근 사회전반에 걸쳐 SW의 사용과 의존성이 급증하고 있다. 이에 따라, SW 개발보안 적용 필요성도 대두되고 있다. 과거에 비해, 보다 다양한 분야에서 많은 양의 SW SW의 개발과 활용이 급증하게 됨에 따라, SW 자체의 취약성 및 피해발생도 증가하고 있다. 기존 조사결과[2,3]들에 따르면, SW에서 발생하는 취약점의 60%는 SW개발단계의 프로그래밍 오류에서 발생하게 되는 것으로 알려져 있다.[1,2,3] 이러한 SW의 프로그래밍 오류와 취약점들은 SW 주요 취약점 점검 목록과 취약점 사실 표준인 CWE(Common Weakness Exposure)[16], CVE(Common Vulnerability Exposure)[15] 등에서 확인이 가능하다. SW 운영단계 오류 수정은 설계단계 대비 급증하는 것으로 알려져 있으며, 개발보안 적용을 통해, 보안 취약점들이 20~40%, 감소되는 것으로 알려져 있다.[1,2,3] 최근 국내 공공기관의 정보체계에 대한 SW 취약점 보호 대책은 행정안전부 고시에 의해 공공기관 정보체계에 한해 감리단계 SW 개발보안 의무 적용이라는 항목으로 제도화되었다.[1,2,3] 그러나, 날로 발전해가고 파괴력이 증가하고 있는 사이버전에 대응하여 보안이 중요한 국방 SW분야, 특히 무기체계 내장형 SW에 대해서는 그 광범위성과 일반의 오해와 무지로 인해, 정의나 분류도 명확하지 않은 상태이다. 또한, 명칭이 무기체계 내장형 SW라는 이유로 인해, 현재까지 정부 주도의 SW 개발보안 적용 제도에서 적용대상이 되지 못한 실정이다. 이에 따라, 본 연구에서는 현재 정부 SW개발보안정책에서 논의되고 있지 못한 무기체계 내장형 SW에 대한 개발보안과 시큐어 코딩의 적용 방안에 대하여 논의하고자 한다.

2. 개발 보안 관련 기존 연구

2.1 SW 개발 보안과 시큐어 코딩의 개념

SW개발보안이란, SW 개발과정에서 개발자의 실수나 논리적 오류 등으로 인해, SW가 가질 수 있는 보안취약점과 보안약점을 최소화하기 위해서 설계부터 보안을 고려하여 개발하는 일련의 보안활동과 과정을 의미한다. 넓게는 SW 개발주기상의 각 단계별로 요구되는 모든 보안활동을 포함하고, 좁게는 SW 개발과정에서 소스코드 구현상의 보안약점을 제거하는 시큐어 코딩을 의미하고 있다.[2,3] 이와 관련하여, 국내외의 사례를 살펴보면, 미국의 경우, SW 개발보안의 중요성을 인식하여, 미국 국토안보부(DHS : Department of Homeland Security)가 SW개발 전체 과정에 대한 보안활동 연구를 활발히 진행해오고 있다.[1] 또한 미국표준기술연구소(NIST : National Institute of Standards and Technology)[16]의 표준제정 활동을 통해, 각 단계별 활동과 절차가 표준화되고 있어, 연방정보 정보시스템 구축과 운영 시에 활용하고 있다.[1]

미국의 경우 국방 분야에서는 美 국방 정보체계보호인증사업(DITSCAP : DoD IT Security Certification and Accreditation Program 2000)과 美 연방 정부 기관 정보시스템보호연방정보보안관리법(FISMA:Federal Information Security Management Act of 2002)을 통해서, SW의 개발 단계 시큐어 코딩 적용과 보안적합성 인정 기준 운영을 명

시하고 있다. 일본의 경우, 정부기관 정보보호 대책 통일 기준을 제정하고, 각 기관은 전자정부도입업무를 수행 중이다. 시스템 개발 시, 제안요청서, 소스코드 등에 대해 개발 전 순기에 걸쳐 일관성 확보 및 형상관리절차 자동화를 요구하고 있다.[1]

우리나라의 경우, 행정안전부 SW 개발보안 가이드와 보안과 SW 보안약점 진단 가이드를 2011년 최초 제정하였고, 2012년 행정안전부 고시를 통해, 공공기관 SW에 대한 개발보안 적용 의무화가 시작되었다. 이번 행정안전부 고시의 내용에서 다루는 개발보안과 시큐어 코딩의 내용은 주로, 행정안전부 전자정부 표준프레임 워크를 지원하기 위한 개발보안과 보안약점의 진단 가이드의 성격을 가진다. 때문에, 그 구성과 내용을 살펴보면, JAVA Spring 기반의 웹서비스 환경을 중심으로 구성되어 있으며, 대표적으로 6개 취약점 특성 그룹과 43개의 취약점 대비 코딩룰을 가지고 있다.[2,3] 행정안전부에서 제시하는 개발보안가이드는 기본적으로 기존의 CWE(Common Weakness Exposure)[15], CVE(Common Vulnerability Exposure)[16], SANS Top 25 Software Errors에서 정립된 내용을 공통적으로 잘 반영하고 있다. 다만, 그 관심 적용 분야가 웹기반 행정망이라는 점이 무기체계 내장형 SW와는 범위가 다른 문제가 있다. 행정안전부 가이드에서는 세부적으로는 C 시큐어 코딩 가이드, 자바 시큐어 코딩가이드, 안드로이드 자바 시큐어 코딩 가이드를 구분하여, 제시하고 있다. C와 자바의 경우 언어적 특성에 대한 코딩룰을 20가지 정도 보충하고 있다.[4,11,12] 그러나, 행정안전부안 자체가 큰 틀 자체가 최근 정보체계의 주요한 흐름인 웹서비스를 중심으로 감안한 한계로 인해, 내장형 SW분야에는 적용이 제한되게 되고 있다. 그러므로, 사이버전에 대응한 무기체계 내장형 SW의 개발보안을 위한 시큐어 코딩룰을 별도 적용방안을 마련하는 것이 필요하다.

2.2 주요 시큐어 코딩 룰

현재, 범용으로 개발보안에 적용되는 시큐어 코딩의 룰로는 CERT-C(Computer Emergency Response Team), MISRA-C (Motor Industry Software Reliability Association) 등이 있다,[1] CERT-C는 12개 취약성 특성 그룹과 취약점 대비 코딩 룰 221개로 이루어 져 있다.[15] 이는, 일반적인 C 프로그래밍 코딩룰과 베스트 프랙티스라고 할 수 있다.[1] 반면, MISRA-C는 자동차 공업 분야에서의 SW 신뢰성향상을 위해 제정된 개발표준이다. 자동차 산업 내장형 SW 분야를 중심으로 개발되었으나 그 실용성이 인정되어, 항공/우주, 열차, 국방 분야 등으로 그 적용 범위가 확대되었다. 현재 통용되고 있는 MISRA-C 1998은 총 127개의 룰, 93개의 필수 룰과 34개의 권고 룰을 가지고 있으며, 개정 버전인 MISRA-C 2004는 21개의 취약점 특성 그룹과 총 141개의 취약점 대비 코딩룰로 구성되어 있으며, 적용 수준에 따라, 121개의 필수 적용 룰과 20개의 권고 적용 룰로 구분되어 있다.[1] MISRA-C 코딩룰은 고가로 판매되고 있어, 일반적으로 공개되어 있지는 않은 한계가 있다. 때문에, 이를 구입하지 못한 일반에서는 이에 대한 참조를 MISRA-C 코딩룰을 재해석한 것으로 알려져 있는 JSF AV C++을 통해 하고 있는 실정이다.

앞서 2.1절에서 언급된 바와 같이, 국내에는 행정안전부에서 제정한 C 시큐어 코딩 가이드, 자바 시큐어 코딩가이드, 안드로이드 자바 시큐어 코딩 가이드가 있다. 이들은, 기존 취약점 리스트와 CERT-C, MISRA-C를 기본적으로 참고는 하고 있으나, 제정과정

에서 적용항목 선정이 주로 행정전산망 정보보호를 위한 웹서비스 요소를 중심으로 개발되었다. 단적인 예를 들면, 행정안전부 코딩룰의 경우 CERT C와 MISRA C가 다루고 있는 100~200개 이상의 룰에 비해, 달리 코딩룰이 언어별로 40~50개 정도로 축약되어 있다. 한편, 국내 개발보안에서 활용되고 있는 시큐어 코딩의 주요영역과 핵심은 주로 10가지 항목으로 설명되는데, 입력되는 값의 확인, 컴파일러의 경고 주의, 보안정책의 구성과 적용. 프로그램과 코드의 단순성 유지. 기본 거부 원칙. 최소 권한 부여 원칙. 불필요한 데이터 전송 노출 제한. 여러 단계에 걸친 보안 확인 적용. 보안 기법의 효율화. 시큐어 코딩 표준 사용이 주요 고려 항목으로 권장되고 있다.[2,3]

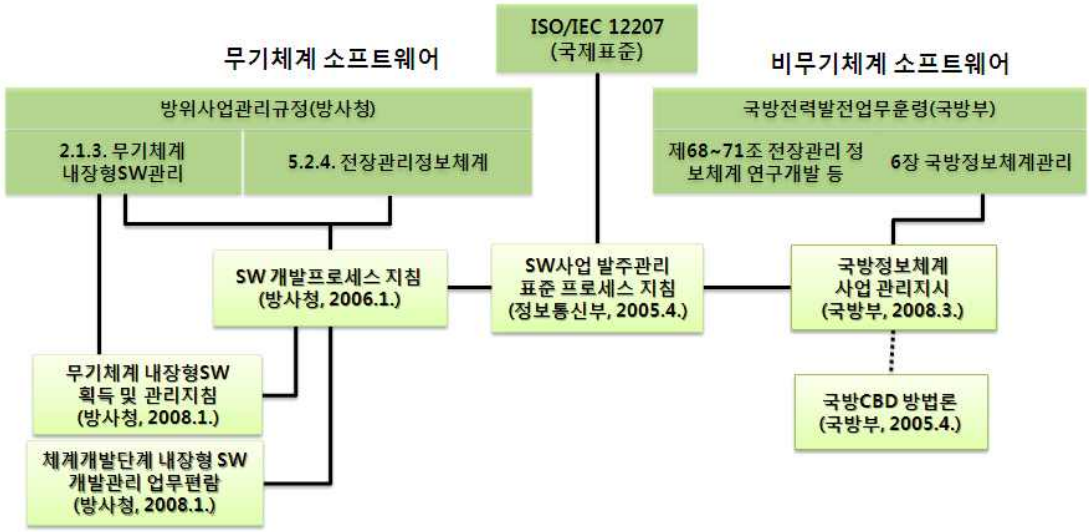
본 연구의 주안점은 현재 행정전산망 정보체계를 중심으로 도입되기 시작한 개발보안 적용을 국방SW와 무기체계 내장형 SW에도 적용 가능한 방안을 제시하는 것이다. 이를 통해, 향후 NCW 전장 환경에서 중요한 사이버전에서 발생할 수 있는 무기체계 내장형 SW 의 각종 문제들, 생존성과 운용연속성, 신뢰성, 기밀성, 가용성, 비밀성이 유지할 수 있는 방안을 마련하는 것이다. 그러므로, 본 연구에서 특정 시큐어 코딩룰을 세부적으로 설명하거나 적용사례를 설명하는 것, 또는 새로운 시큐어 코딩룰 자체를 제정하는 것은 연구의 범위를 넘어설 뿐 아니라, 너무나 방대한 양이므로 불가능하다. 예를 들어, 행정안전부에서 재정한 개발보안적용지침의 경우, 한국인터넷진흥원(KISA : Korea Internet and Security Angecy)과 시큐어 코딩 관련 전문 업체와 테스팅 전문 업체를 통해, 장시간에 걸쳐 기존 미국 사례를 중심으로 연구하여 도출한 적지 않은 양의 결과물이다. 또한 각각의 시큐어 코딩을 해설하는 서적들이나 보안가이드의 분량도 적지 않다.

2.3 현행 국방 SW 관련 규정 요건

우리나라의 현행 국방 SW 관련 규정들은 SW 개발보안이나 시큐어 코딩을 별도로 정의하고 있지 않다. 그러나, 무기체계 SW 신뢰성 관련 규정에서는 “무기체계 내장형 SW 신뢰성은 무기체계 내장형 SW가 실제 무기체계 작동환경에서 무기체계 운용 기간 동안 사용자 요구사항에 제시된 기능을 반복적으로 수행 시 정확하고 일관성 있게 작동할 수 있는 SW 능력”임을 언급하면서, SW가 가지고 있어야할 보안성의 필요성을 규정하고 있다.[5] 또한, 무기체계 SW 품질 관련 규정에서는“SW 품질은 주어진 요구를 만족하기 위한 능력에 영향을 미치는 SW 제품의 모든 특성과 속성들로 SW 평가를 위한 품질특성들과 메트릭 정의”[5]임을 언급하고 있는데, 이는 ISO9126의 기능성 항목과 연계되어, 명시적이지는 않지만, 보안 필요성을 내재하고 있는 것으로 해석해야만 한다.[1]

한편, 무기체계 상호운용성 측면에서는 “상호운용성 관리지침 제56조(정보보호 대책 수립)에서 ① 사업관리본부장(통합사업팀장)은 연구개발사업 및 구매사업에 대한 무기체계에 대하여 불법 사용자로부터 침해대응과 안전한 군사작전 수행하기 위하여 상호운용성 확보방안 수립 시 기밀성, 무결성 및 가용성을 바탕으로 정보보호 대책을 수립하여야 한다.”[6] 임을 명시하고 있어, 보안 필요성을 언급하고 있다.

결과적으로 현행 규정들은 SW개발보안이나 시큐어 코딩에 대한 요구사항이나 적용 필요성과 적용 수준 등을 명시하고 있지만 않을 뿐 SW 보안성 요구는 기본적으로 내재되고 있는 것으로 해석해야만 한다. 현재 국방 SW와 관련된 규정의 이해를 위해 이들을 종합하여 도식화하면 <그림 1>과 같다.



<그림 1> 국방 SW 및 무기체계 내장형 SW 관련 현행 규정 체계

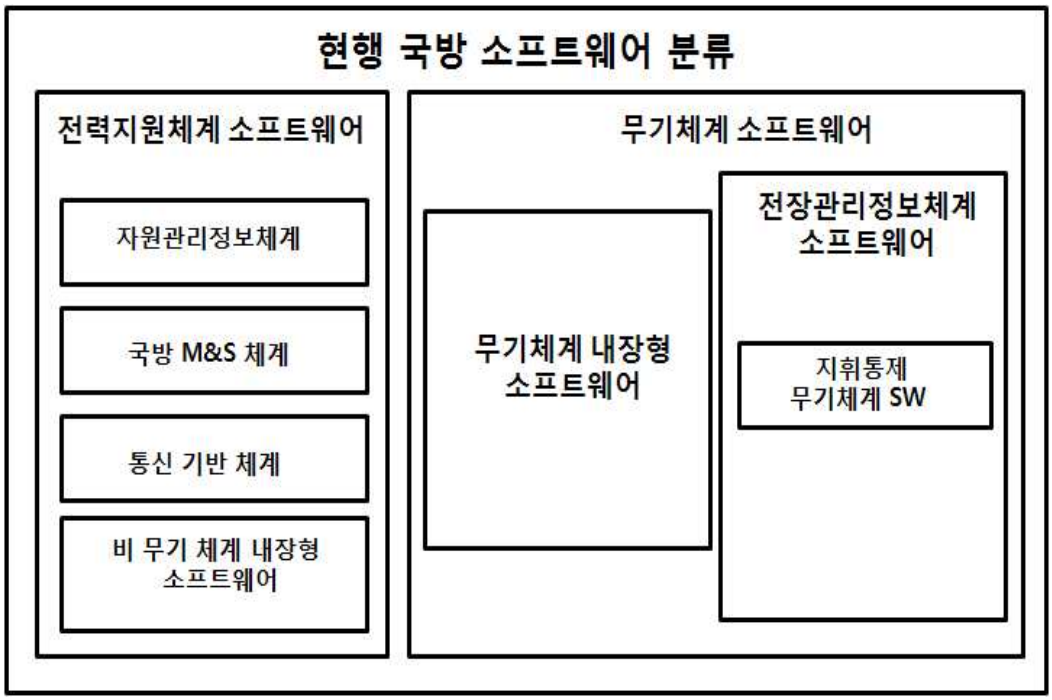
출처 : 장영근, 항공대학교, 2012, 군용항공기 감항 인증 SW 기능 검증 관련 발표 자료

현행 국방 SW 분류에서는 일반 SW나 정보체계로 분류하는 SW자원들이 자원관리 정보체계, 국방M&S체계, 전장관리정보체계, 지휘통제 무기체계로 세분화하고 있다. 또한 무기체계 SW 분야에서 무기체계 내장형 SW와 전장관리정보체계 SW라는 일반에서 이해하기 어려운 분류체계를 볼 수 있으며, 전력지원체계 SW에 비무기체계 내장형 SW라는 별도 항목을 볼 수 있다. 국방 SW 분야의 용어 사용의 이러한 차이, 구분의 복잡성, 개념상의 차이들로 인해, 일반 분야와는 달리 여러 가지로 혼란이 발생 할 수 있다. 현행 국방 SW의 분류체계를 현행 규정들에 따라 도식해보면 아래 <그림 2>와 같다.

3. SW 개발 보안 적용 방안

3.1 전력지원체계 SW에 대한 개발보안 적용 방안

국방 SW 와 관련된 규정들을 기준으로 SW개발보안, 즉 시큐어 코딩의 적용 수준과 현행 정부고시안의 적용방안을 알아본다. 국방SW 중 자원관리정보체계와 국방 M&S 등의 체계의 경우에는 이름만 국방일 뿐이고, 일반에서 널리 사용되는 사무용 일반 정보체계의 성격과 크게 다를 바가 없다. 게다가 그 구성도 웹서비스 형태이고, 일부의 경우에는 이미 설계 및 구현단계에서부터 정부 표준인 전자정부 프레임워크를 채택하고 있다. 그러므로, 국방SW 중 자원관리정보체계와 국방 M&S 등의 체계의 경우에는 전자정부 프레임워크 기반의 개발보안 적용방법론 성격을 갖는 행정안전부 개발보안지침과 코딩룰을 활용하면 큰 무리가 없을 것으로 판단된다.



<그림 2> 국방 SW 분류 (현행 국방 SW 관련 규정을 종합하여 도식화)

다음으로, 통신기반체계와 비무기 체계 내장형 SW는 국방용으로 개발된 것이 아니라, 상용제품을 내장된 것을 용도만 국방용으로 활용하는 것을 의미한다. 이런 경우들은, 일종의 패키지 SW와 같이 별도의 개발보안 적용은 제한된다고 보아야 하며, 미국의 경우처럼, 국방 분야에서 사용되는 모든 장비와 이들에 포함되는 모든 SW가 美 국방 정보체계보호인증사업(DITSCAP : DoD IT Security Certification and Accreditation Program 2000)에 의해 검증되고 있음을 감안하면, 우리도 우리 실정에 맞는 패키지나 일반 도입 하드웨어에 적합한 보안성 검증 수단을 구축하여 적용할 필요가 있다. 제2차 이라크전의 경우, 이라크군 지휘통제망에 연결된 PC와 프린터 등의 기기들에 논리폭탄이 내장되어 이라크군의 지휘통제망 교란에 활용된 사례가 있다. 우리 국방분야에서도 이런 사례는 더 이상 남의 일이 아니므로 정보체계 보호인증 방안 역시 필요한 부분이다. 그러나, 이 부분은 본 연구의 개발보안 적용방안의 범위로는 적합하지 못하므로 향후 별도 연구에서 다루고자 한다.

3.2 무기체계 SW에 대한 개발보안 적용 방안

국방 SW 개발보안 적용에서 가장 문제가 될 것으로 예상되는 분야는 일반 사무환경이 아닌 전장 환경 운영에 직접적으로 관련되는 무기체계와 관련된 SW 즉, 무기체계 내장형 SW와 전장관리정보체계 SW 분야이다. 이 분야만이 국방 SW 중 실제로 국방에 전용되는 특성을 갖는다.

1) 전장관리정보체계 SW에 대한 개발보안 적용 방안

전장관리정보체계 SW 중, 대표적인 체계인 C4I체계의 구현 SW들은 초기에는 클라이언트/서버(Client / Sever) 방식이었다. 그러나, 2000년대 이후 개발된 각군 전술 C4I를 비롯한 KJCCS(Korean Joint Command and Control System)를 비롯한 최근의 지휘소 C4I체계들은 기본적으로 국방 CBD(Component Based Development) 방법론을 활용하고, 서비스 방식에 있어서는 웹서비스(Web Service) 방식을 채택하고 있다.

그러므로, 현재 전력화되어, 통용되는 전장관리정보체계들은 웹서비스(Web Service) 성격을 가지는 것으로 볼 수 있다. 또한, 향후 발전 방향이 SOA(Service-Oriented Architecture)이므로, 구현 방식에 있어서 현재와 큰 변화와 차이는 없을 것으로 예상된다. 향후 변화양상에는 활용 플랫폼에 있어서는 스마트 디바이스가 활용될 수 있다는 정도의 차이만이 있을 것이다. 그러므로, 전장관리정보체계의 경우에도, 향후 성능개량으로 추가 개발되는 경우이거나 재개발 하는 경우에 전자정부 프레임워크 기반을 반영하는 전자정부 개발보안 지침을 적용하면 된다. 현재 전력화 되어 활용 중인 체계들의 경우에는 이미 개별적으로 개발된 사항이므로, 개발보안 적용대상이 아니며, 국내외의 경우들을 살펴보면, 대부분의 경우 기존(Legacy) 체계에 대해서는 개발보안 적용 의무화는 실시하지 못하고 있고, 점차적으로 도태시키는 것을 방안으로 채택하고 있다.

2) 무기체계 내장형 SW에 대한 개발보안 적용 방안

무기체계 내장형 SW는 각종 무기체계에 내장되어 해당 장비의 임무 수행에 전용으로 제공되는 SW를 의미한다. 또한, 무기체계 고유 하드웨어를 제어하는 기능을 제공하는 경우, 모두 무기체계 내장형 SW로 분류하기 때문에, 일반적인 내장형 SW보다 규모가 큰 경향이 있다.[1,5]

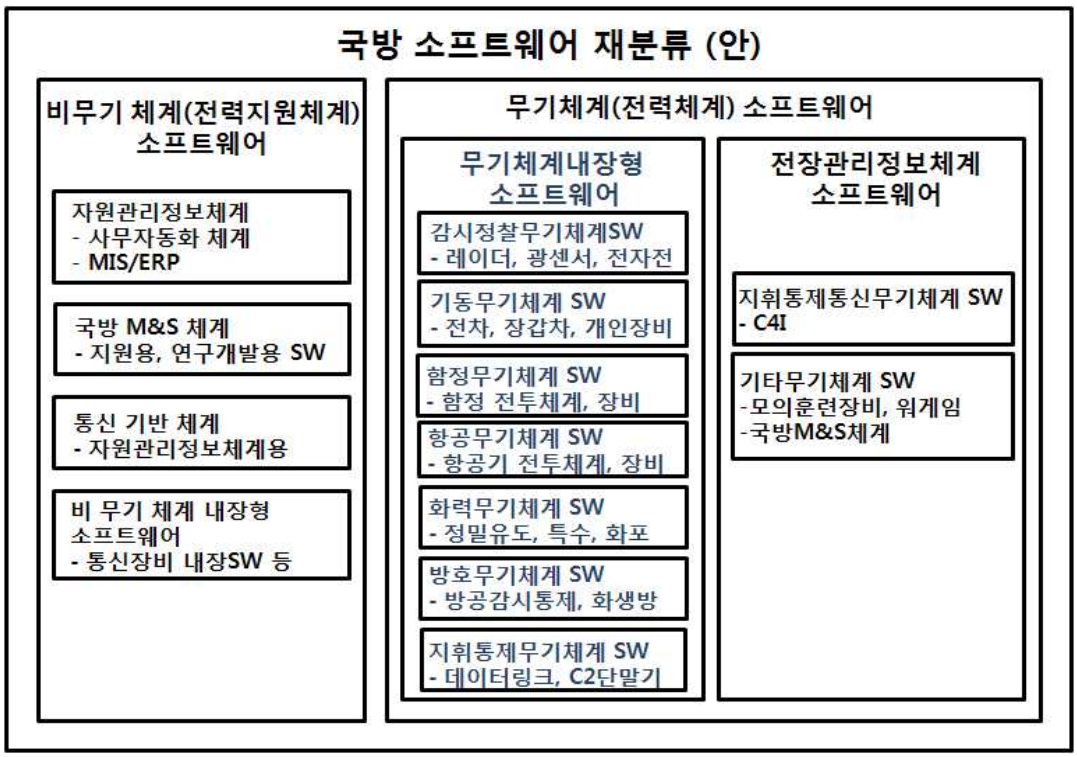
일반적으로, 국방 SW에 대한 개발보안 적용 시 예상되는 문제점들은 일반적인 정보체계사업과도 유사한 부분과 특이한 부분으로 나누어 질 수 있다. 일반적인 사항은 잦은 요구사항 추가와 설계 변경, 시험 단계에서 요구사항 추가 같은 사항, 개발자/설계자 역량 차이와 개발보안 실제 적용 여부 등이다.

무기체계 내장형 SW만이 갖게 되는 고유한 문제점은 기존 시큐어 코딩룰의 적용 체계별 적합성 여부이다. 무기체계SW와 무기체계 내장형 SW의 경우 각 체계의 범위가 워낙 넓어 체계의 특성이 다양하여, 일괄적인 적용이 제한된다. 그러므로, 현재의 무기체계 SW와 무기체계 내장형 SW 분류를 상세하게 재분류하는 것이 선행되어야만 한다.

무기체계 내장형 SW의 특성에 따른 개발보안 적용을 위해서는 이러한 분류체계에 의하여 무기체계와 무기체계 내장형 SW를 재분류하고, 각 분야별로, 적용수준을 차등화하는 것이 필요하다. 현재 무기체계 내장형 SW에 개발보안 적용 시에, 가장 문제가 되는 것은, 내장형 SW에 대해서는 행정안전부에서 제정한 JAVA, 안드로이드 JAVA 가이드를 제외하고는 이렇다 할만한 참고 자료가 없다는 점이다. 그러나, 현재 무기체계 개발에서 있어서, 무기체계 내장형 SW 중 JAVA나 안드로이드 JAVA의 비중은 그리 높지 않다. 현재 대부분의 무기체계 내장형 SW는 C 또는 C++로 개발되고 있어, 국방분야의 무기체계 내장형 SW 개발에는 기존 정부 지침의 활용이 어렵다.

이에 대한 해소 방안으로는, 기존의 주요 코딩룰을 조합한 슈퍼세트를 구성하고, 위 제안에서 사용한 8대 무기체계 분류별로 세부 코딩룰을 구성하는 것을 고려할 수 있다.

이러한 방안의 적용에는 무기체계별 성격을 고려하여, 각 분야를 재분류하고 시큐어 코딩룰 적용 수준을 결정해야 한다. 또한, 이 과정에서 고유 특성과 운용 환경 고려한 시큐어 코딩을 적용해야한다. 예를 들어, 감시정찰무기체계 내장형 SW의 경우에는, 광센서나 레이더 등의 센서는 내장형 SW로써, 행안부 시큐어 코딩룰만 적용하기 어렵다. 그러므로, 각각의 내장형 SW에 적합한 코딩룰을 CERT C와 MISRA C등을 참조하여 별도의 국방 무기체계 내장형 SW 코딩룰 세트를 제정할 필요가 있다. 현행 8대 무기체계 분류 방식을 따라 국방 SW와 무기체계 내장형 SW의 관계를 나타내보면 아래 <그림 3>와 같다. <그림 3>의 국방 소프트웨어 재분류(안)은 본 연구에서 제안하는 세분화된 국방 SW와 무기체계 내장형 SW의 새로운 분류체계이다.



<그림 3> 국방SW 개발보안 적용을 위한 분류 체계(안) (체계별 특성 고려 세분화)

기동 무기체계 내장형 SW, 함정 무기체계 내장형 SW, 화력 무기체계 내장형 SW의 경우에는 기존의 CERT C와 자동차/항공/철도에서의 산업표준인 MISRA C를 사용하는 것이 타당할 것으로 보인다.

한편, 항공무기체계 내장형 SW의 경우에는, 별도로 요구되고 있는 안정성 적합인증 수단인 DO178-B 또는 DO178-C(DO-178 : 항공분야의 SW 안정성 적합인증 상용표준이나, 항공우주산업계의 사실 표준 ; RTCA社 Software Considerations in Airborne Systems and Equipment Certification) 기준에 부합한 인증 적용이 필수적인 항목이다.

그러므로, 이 항목을 제외할 수가 없다. 항공 무기체계 관련 분야에서도 C안정성이 보장된 CERT C와 MISRA C를 선별 적용하는 것이 타당할 것이다.

지휘통제무기체계 내장형 SW와 방호무기체계 내장형 SW의 경우에는 타 체계에 탑재 되는 부체계가 되는 경우도 있고, 그 자체가 단말기가 되는 경우도 있다. 그러므로, 분류가 더욱 애매한 면이 있다. 단말기의 경우, 행정안전부의 안드로이드 자바 코딩룰, C 코딩룰, 자바 코딩룰을 기본적으로 준용하고, CERT C 코딩룰로 보충하는 방식이 타당할 것으로 보인다. 반면, 정보체계성격을 갖는 지휘통제무기체계나 방호무기체계의 경우에는 웹서비스 기반인 경우, 행정안전부 기준의 웹서비스 관련 시큐어 코딩 룰들을 적용하는 것이 타당할 것이다. 다음의 <표 1>는 본 연구에서 앞서 제안하고 있는 현행 8대 무기체계 분류의 따른 무기체계 내장형 SW별 적용 수준을 정리한 것이다.

<표 1> 8대 무기체계 분류에 따른 무기체계 내장형 SW 시큐어 코딩 적용 수준 (안)

현행 8대 무기체계별 분류 (안)	무기체계별 시큐어 코딩 적용 수준 (안)
감시정찰무기체계 내장형 SW – 레이더, 전자광학기기 센서류, 전자전 장비	MISRA C / CERT C 수준 적용
기동무기체계 내장형 SW – 전차, 장갑차의 차량 전자체계와 발사 장치, 사격통제장비, 지휘통제통신장비	MISRA C / CERT C 수준 적용 KISA/행정안전부 지침 필요시 적용
함정무기체계 내장형 SW – 수상함, 잠수함의 운항체계와 전투체계, 지휘통제통신장비	MISRA C / CERT C 수준 적용 KISA/행정안전부 지침 필요시 적용
항공무기체계 내장형 SW – 항공기 전투체계와 단위 구성품, 지휘통제통신장비	DO178 B,C 적용 MISRA C / CERT C 수준 추가 적용
화력무기체계 내장형 SW – 정밀유도무기, 화포 등에 탑재된 유도장치, 발사 장치, 사격통제장비	MISRA C / CERT C 수준 적용
방호무기체계 내장형 SW – 방호장비, 방공관제통제 장비, 사격통제장비, 지휘통제통신장비	KISA-행정안전부 지침 적용 MISRA C / CERT C 수준 추가 적용
지휘통제무기체계 내장형 SW – 상호운용성 기반, 데이터링크, 개별통신 장비, 탑재형 데이터통신 장비	플랫폼별 요구수준에 따라 차등적용 DO178 B,C / MISRA C / CERT C

한편, 이 과정에서, 우선순위 산정을 위해 정량적 평가를 위한 체계별 치명도, 위험도 산정의 과정을 사전에 정립하는 것도 필요하다. 왜냐하면, 기존에 별도 기준이 없는 사항에 대한 평가이므로, 관리를 위해서는 측정 평가 수단이 필요하기 때문이다. 치명도와 위

험도 산정 방법론을 준용한 적용 요구 수준 평가에는 무기체계 SW별 체계에서의 보안 위험 영향도 평가하는 것이 우선적으로 필요하다. 또한, 위험도에 따른 테스트 대상 식별 및 우선순위 결정 수단도 필요하다.[1] 다음 <표 2>은 무기체계 SW 치명도와 위험도 평가요소에 대한 본 연구에서의 제안이다. 그러나, 치명도, 위험도 산정에 대한 보다 구체적이고 상세한 연구는 본 연구의 범위를 넘게 되므로 향후 별도의 연구에서 다루고자 한다.

<표 2> 무기체계 내장형 SW에 대한 치명도와 위험도 평가요소 제안

무기체계 내장형 SW 치명도 평가 요소 (안)	무기체계 내장형 SW 위험도 평가 요소 (안)
- 무기체계 SW 기능 - 무기체계 SW 성능 - 무기체계 SW 신뢰성 - 무기체계 SW 안정성 - 무기체계 SW 개발 비용 - 무기체계 SW 개발 기간	- 무기체계 SW 적용 기술 성숙도 - 무기체계 SW 복잡도 - 무기체계 SW 요구사항 - 무기체계 SW 안정성 - 무기체계 SW 테스트 - 무기체계 SW 개발자의 수준

3) 무기체계 내장형 SW 개발보안 적용 추진 방안

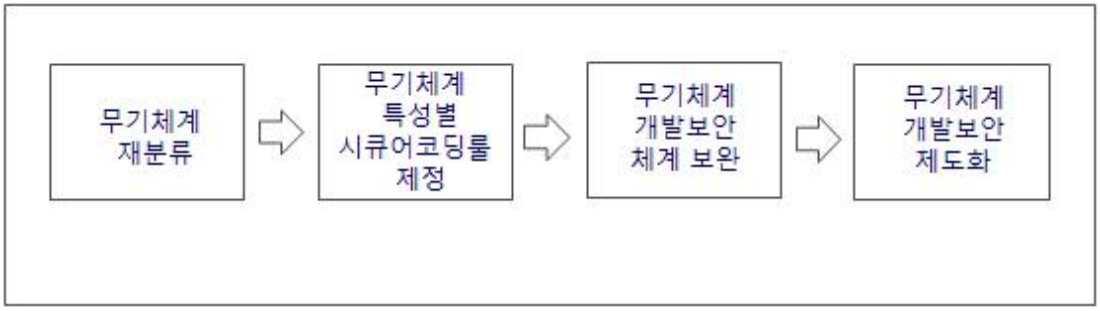
무기체계 내장형 SW는 특정 무기체계 하드웨어를 조종 또는 운용한다는 특성으로 인해 현재 정보체계 감리대상에서 제외되어 있다. 그러므로, 감리대상 SW를 대상으로 의무화를 명시한 현행 행정안전부 개발보안 지침과 행정안전부 고시의 적용대상은 될 수 없는 상황이다.

반면, 무기체계 내장형 SW를 관장하는 국방 SW 관련 규정들은 개발보안의 필요성은 언급하고 있는 실정이다. 현행 제도상으로 무기체계 내장형 SW의 개발보안은 필요는 하지만, 적용할 방법은 없는 실정이다.

최근 무기체계 내장형 SW의 신뢰성 문제로 인해, 무기체계 내장형 SW 신뢰성에 대한 방위사업청의 연구 용역이 실시된 바 있다. 그러나, 무기체계 내장형 SW 신뢰성 향상 적용 방안에 대해 업계 입장은 매우 부정적이었다. 무기체계 내장형 SW 신뢰성 향상 적용 방안에서 매우 긍정적인 요소들이 많이 언급되었으나, 실제 업계에서 수긍하기 어려웠던 이유는 기존의 광범위한 각 무기체계들에 적용된 모든 기법들은 통합하여, 모든 무기체계에 동일하게 적용되는 것 같은 인상을 주었기 때문이다.

같은 관점에서 보면, 개발과정에서 새로운 제도나 규정의 적용은 개발자 입장에서 매우 번거로운 일이다. 즉, 추가적인 비용과 시간의 소요가 발생하는 것으로, 이런 제도의 적용에 대해서, 자발적인 적용을 기대하기는 어렵다. 그러므로, 명확한 적용 수준과 지침의 개발이 선행되어야만 한다. 그러므로, 본 연구에서는 향후 사이버전에 대응한 무기체계 내장형 SW 개발보안 적용에 관련하여 아래 <그림 4>과 같이 무기체계 내장형 SW 개발보안 적용을 위한 단계별 추진 방안을 제안하고자 한다. 무기체계 내장형 SW에 대한 개발보안 적용은 현재까지 고려되지 않았던 사항이므로, 우수 사례만을 적절하게 모방한다고 하여도, 향후 준비와 적용에는 최소 3년 이상의 준비 기간이 필요할 것으로 예

상된다. 이 과정에서 먼저 현행 무기체계와 향후 무게체계를 명확하게 재분류하는 것이 필요하다. 다음으로, 특히, 가장 중요한 단계는 각 무기체계별 특성에 적합한 무기체계별 시큐어 코딩룰의 제정이 필요하다. 다음으로는, 시큐어 코딩룰을 포함한 무기체계 개발보안과 관련된 제도 체계를 여러 가지 측면에서 충분히 고려하여 구축하여야 한다. 기존 일부 제도들이 시행 후 보완하는 과정에서 생긴 오류들을 반복할 필요는 없기 때문이다. 그러므로, 충분한 검토 시간을 가진 뒤 제도화하는 것이 타당할 것이다.



<그림 4> 무기체계 내장형 SW 개발보안 적용 단계별 추진 방안 제안

4) 무기체계 내장형 SW 개발보안 적용 기대효과

무기체계 내장형 SW에 대한 개발 보안의 적용의 기대 효과로는 무엇보다 먼저, 무기체계 내장 SW 보안취약성을 활용한 무기체계 무단권한획득 방지를 들 수 있다. 현재 지능형 지속위협 등의 보안 위협들은 사회전반에 퍼져 있으며, 향후 사이버 전장의 지휘통제 전용망도, 보안위협에서 안전할 수 없다. 특히, 무기체계에 대한 무단권한 획득이나, 운용연속성과 생존성, 신뢰성을 저하시키는 위협행위들에 대한 대책이 시급하다.

무기체계 내장형 SW에 대한 개발 보안의 적용의 부수적인 효과로는 무기체계 내장형 SW 품질의 향상, 무기체계 내장형 SW 신뢰성의 보장, 무기체계 내장형 SW의 상호운용성 요건 충족, 무기체계 내장형 SW 오류와 대응 비용 감소 같은 긍정적인 요소들을 기대할 수 있다. 그러므로, 향후 무기체계 내방형 SW 개발에 있어서, 개발 단계에서부터 개발보안을 추진하는 것이 필요하다.

4. 결론

본 연구에서는 향후 개발보안 적용에 필요한 국방 SW와 무기체계 내장형 SW에 대하여 각각의 SW를 분류하고, 개발보안의 적용방안과 고려요소를 제시하였다.

향후 NCW 전장 환경에 의해 전쟁 양상이 사이버전의 양상을 띄고 있다. 이에 따라, 국방 전반의 SW, 특히 무기체계 내장형 SW의 보안성의 중요성과 필요성이 분명함에도, 무기체계 내장형 SW에 대한 개발보안과 시큐어 코딩이 논의되지 않은 문제가 있다.

무기체계 내장형 SW에 대한 보안위협은 지속적으로 가중될 것이므로, 본 논문은 시의적인 가치가 있다 할 수 있다.

특히, 무기체계 내장 SW 개발 보안 적용 기대 효과로는 무기체계 내장 SW 보안취약성을 활용한 무기체계 무단권한획득 방지와 SW 품질, 신뢰성, 상호운용성 요건 충족, SW 오류와 대응 비용 감소 같은 긍정적인 요소들이 많이 있으므로, 개발보안을 적절하게 추진하는 것이 필요하다.

향후 연구는 각 무기체계별 고유 특성과 코드에 따른 발생 가능 취약점들을 구체적으로 도출하고, 각 무기체계별 특성에 적합한 특성화된 시큐어 코딩룰들을 구체화하여 개발하는 것이 필요하다.

각 무기체계에 적합한 시큐어 코딩룰의 제정은 개인이 할 수 있는 작업이 아닌 관계로, 공공기관 차원에서 보다 많은 관심과 투자가 필요하다. 또한, 이 과정에서, 우선순위 산정을 위해 정량적 평가를 위한 체계별 치명도, 위험도 산정의 과정을 사전에 정립하는 것도 필요하다.

참고문헌

[1] 최준성, 김우제, 국광호,“무기체계 내장형 SW 개발보안 적용방안”, 2012 한국경영과학회 추계학술대회 / 방위사업청 무기체계 시험평가 세미나 논문집, pp1454-1466, 2012
[2] SW 개발보안 가이드, KISA/행정안전부, 2012
[3] SW 보안약점 진단가이드, KISA/행정안전부, 2012
[4] C 시큐어 코딩 가이드, KISA/행정안전부, 2012
[5] 무기체계 내장형 SW 획득 및 관리 실무지침서, 방위사업청, 2011
[6] 상호운용성 관리지침, 방위사업청, 2012
[7] 방위사업관리규정, 방위사업청, 2010
[8] 국방전력발전업무훈령, 국방부, 2011
[9] 무기체계 SW 개발 및 관리 지침, 방위사업청, 2011
[10] 정보시스템 구축운영 지침, KISA/행정안전부, 행정안전부, 2012
[11] JAVA 시큐어 코딩 가이드, KISA/행정안전부, 2012
[12] 안드로이드 JAVA 시큐어 코딩 가이드, KISA/행정안전부, 2012
[13] CWE, MITRE, http://cwe.mitre.org
[14] CVE, MITRE, http://cve.mitre.org
[15] CERT Secure Coding Standard, http://www.securecoding.cert.org
[16] NIST, http://www.nist.gov