정 보 보 호 학 회 지
제26권 제1호, 2016. 2

소프트웨어 보증을 위한 국내 시험·인증 동향 및 발전방향

방 지 호*, 지 재 덕**

요 약

최근 빈번하게 발생하는 사이버침해사고에 대한 대응 방법이 네트워크 및 호스트 기반의 정보보호제품 도입·구축·운영에서 사이버침해사고의 근본 원인인 취약한 SW에 대한 보증 활동에 집중하는 사전 대응으로 변화하고 있다. 본 논문은 행정자치부 및 KISA의 SW 개발보안 활동을 통해 개발자 측면의 SW보증활동을 소개하고, SW보증과 관련된 국내 SW 시험·인증 동향에 대한 설명 및 발전방향을 제시한다.

Ⅰ. 서 론

소프트웨어(Software, SW) 보증(Assurance)은 SW 생명주기(Life-cycle)동안 의도적으로 설계되었거나 실수로 SW에 포함될 수 있는 보안취약점(Vulnerability)으로부터 얼마나 자유로운지에 대한 신뢰 수준으로, SW가 의도된 방법대로 동작하는 것을 의미한다[1]. SW 보증은 SDLC에 대한 체계적인 접근 방법으로 개발하여 추정된 비용과 기간에 고객이 원하는 품질 높은 SW를 개발하는 다양한 이론, 개념, 기술 등을 다루는 SW 공학을 적용한 활동이라고 할 수 있다. SW 보증은 SW 개발생명주기(Software Development Life Cycle, SDLC)를 기반으로 SW 개발단계별 개발자의 보증 활동으로 얻어질 수 있다.

최근, 빈번하게 발생하는 사이버침해사고에 대한 대응 방법이 네트워크 및 호스트 기반의 정보보호제품 도입·구축·운영에서 사이버침해사고의 근본 원인인 취약한 SW에 대한 보증 활동에 집중하는 사전 대응으로 변화하고 있다. 이는 美 국토안보부(DHS, Department of Homeland Security), 상무부(Department of Commerce)의 국립표준기술연구소(National Institute of Standards and Technology, NIST), 국방부(Department of Defense, DoD), 국가안보부(National Security Agency, NSA) 등 연방정부기관을 중심으로 2003년 2월부터 안전한 사이버공간에 대한 국가정책의 일환으로 추진하고 있는 SW 보증 프로그램이 대표적이다. 미국의 SW 보증 프로그램에는 MITRE 등 정보보안 관련 비영리 연구기관과 OWASP(Open Web Application Security Project), SAFECode(Software Assurance Forum for Excellence in Code) 등과 같은 비영리조직, 학계(카네기멜론대학교 등), 교육기관(SANS 등), IT 개발업체(CISCO, HP, IBM 등) 등 다양한 조직이 참여하여 있으며, SW보증포럼(Software Assurance Forum)[1]을 통해 다양한 SW보증활동에 대한 연구 및 토론을 진행하면서 표준화를 주도하고 있다. 현재 SW보증의 개념에 SW 공급망에 대한 개념을 포함하여 SSCA(Software & Supply Chain Assurance)로 명명하여 활동을 진행하고 있다.

국내의 경우, 2009년부터 행정자치부 및 한국인터넷진흥원을 중심으로 SW보증에 대한 연구를 진행하며 2012년부터 국가 정보화사업시 SW 사업규모에 따라 단계적으로 SW보증 활동을 의무화하도록 하였다. 현재 SW 구현에 대한 보증활동, 즉 시큐어코딩(Secure Coding) 적용을 의무화하였으며 점진적으로 운영, 설계단계 등으로 확대를 추진[2]하고 있으며, 관련 동향은 2장에서 설명하도록 한다.

SW공학에서 SW보증을 위한 전통적인 SW개발방법론으로 폭포수모델(Waterfall), 원형모델(Prototyping),

* (재)한국기계전기전자시험연구원 정보통신산업본부 정보보안평가센터 (jhbang@ktc.re.kr)
** (재)한국기계전기전자시험연구원 정보통신산업본부 정보보안평가센터 (jdji@ktc.re.kr)

나선형모델(Spiral) 등이 대표적이다. 전통적인 SW 개발방법론은 개발자가 SDLC 각 단계별로 개발 및 보증 활동을 수행하며 요구사항 명세서, 설계서, 시험서 등의 산출물을 생성하며 사용자의 요구사항을 올바르고 빠르게 구현하는데 초점을 맞추고 있다. 반면, 마이크로소프트社의 MS-SDL[3](Microsoft Security Development Lifecycle), CLASP[4](Comprehensive, Lightweight Application Security Process), 7 TouchPoint[5] 등과 같은 SW 개발방법론은 전통적인 SDLC와 다르게 SW에 대한 보안위협을 고려하여 보안취약점이 발생되지 않도록 SDLC 단계별로 관련 보증활동을 하도록 하고 있다. 보안을 고려한 SDLC를 적용하여 SW 개발에 대한 효과는 보안 패치율이 감소한 MS-SDL 적용 사례[3]에서 살펴볼 수 있다. 국내의 경우, 전자정부지원사업으로 개발되는 SW를 대상으로 SDLC 단계 중 구현단계에서 시큐어코딩 관점의 SW보증활동을 통해 보안약점(Weakness)이 감소하는 효과[6]가 나타났다. MS-SDL과 국내 시큐어코딩 관점의 SW보증활동의 사례를 통해서 보안을 고려한 SW보증 활동이 안전한 SW 개발에 도움이 되며, 사이버침해사고를 선제적으로 예방할 수 있는 좋은 방법이라고 할 수 있다.

SW보증은 개발자 측면뿐만 아니라, 개발자의 보증활동에 대한 검증을 수행하는 제3자, 즉 시험·인증기관의 활동도 중요하다. 시험·인증기관의 역할은 개발자의 SW보증활동이 적절하게, 즉 보안위협에 대응하는 보안요구사항들이 정확하고 충분하게 도출되었으며, 도출된 보안요구사항들이 SW 설계 및 구현시 정확히 반영되었는지 확인하여 검증하는 것으로 개발자가 SDLC 단계별로 수행한 SW보증활동의 산출물을 기반으로 수행된다. 따라서, SW보증은 개발자의 활동에, 시험·인증기관의 활동이 병행되어야 얻어질 수 있다고 할 수 있다.

본 논문은 개발자 측면의 SW보증활동보다, SW보증과 관련된 국내 SW 시험·인증 동향에 대해 살펴보고 발전방향을 제시하도록 한다.

본 논문은 2장에서는 국내 SW 개발보안 제도에 대해 설명하고, 3장에서는 국내에서 대표적인 SW 시험인증 제도인 정보보호제품 및 신용카드 단말기 대상의 시험인증에 대해 설명한다. 마지막으로, 4장에서 SW 보증의 발전방향을 제시하며 결론을 맺는다.

Ⅱ. 국내 SW 개발보안 제도 추진 동향

국내에서는 2009년부터 사이버침해사고에 대한 근본적인 대책 마련을 위해, 행정자치부 및 한국인터넷진흥원(KISA)를 중심으로 SW에 내재된 보안취약점의 원인인 보안약점을 식별하여 제거하기 위한 다양한 연구가 진행되었다. 이에 대한 결실로, 2012년 12월부터 감리대상 국가 정보화사업 규모에 따라 단계적으로 SW 개발보안이 의무화[2] 되었다. 행정자치부 및 KISA에서 정책적으로 추진하는 SW 개발보안은 SDLC의 구현단계에서 설계, 운영단계로 확대되고 있으며, 다음과 같은 SW보증 활동을 고려하고 있다.

2.1. 요구사항 분석

요구사항 분석은 SW 개발 필요성에 대한 고객의 요구사항을 면밀히 분석하는 단계로, 개발할 SW 기능을 도출하게 된다. 또한, 도출된 SW 기능이 갖추어야 하는 기능 요구사항들을 분석하며, SW 개발에 필요한 SW 개발언어, 개발환경 및 개발플랫폼 등을 정하게 된다. SW 개발보안 관점에서는 개발된 SW가 제공하는 서비스 및 정보(및 데이터)와 운영환경에 대한 보안위협을 분석하여 해당 보안위협에 대응할 수 있는 보안기능 요구사항을 도출하는 단계이다.

개발자는 요구사항 분석 단계를 통해 요구사항 분석서를 생성하고, 해당 문서에 최소한 다음과 같은 내용을 식별 및 기술해야 한다.

가. 개발 대상 SW의 기능 및 제공 서비스 정의
나. SW가 처리하고 제공하는 정보(및 데이터) 식별
다. SW가 동작하는 운영환경
라. SW에 대한 보안위협 분석
마. 식별된 보안위협에 대한 대응방법(예, 보안요구사항) 등

2.2. 설계

설계는 요구사항 분석을 통해 분석된 사용자 요구사항이 오류 없이 유기적으로 잘 동작하도록 SW 기능을 서브시스템, 모듈단위로 세분화하여 SW 기능을 설계하는 단계이다. SW개발보안 관점에서는 요구사항 분석에서 도출된 보안요구사항을 서브시스템, 모듈 설계시 반

영하여 SW기능에 반영될 수 있도록 하는 단계이다. 설계시 카네기멜론대 SW공학연구소(SEI)의 보안설계패턴 등과 같은 보안설계패턴[7,8]을 활용하면 자주 발생하는 설계상의 보안 문제를 해결하는데 도움을 받을 수 있다.

개발자는 설계 단계를 통해 설계문서를 생성하고, 해당 문서에 최소한 다음과 같은 내용을 식별 및 기술해야 한다.

가. 서브시스템 및 모듈 구성과 기능 동작 설명
나. 서브시스템간, 모듈간 상호작용(내외부인터페이스 식별 포함)
다. 서브시스템 및 모듈에 반영된 보안요구사항 설계 내용 등

2.3. 구현

구현은 SW기능을 설계한 대로 주어진 운영환경에서 정상적으로 동작하도록 개발언어 및 개발환경을 선택하여 SW를 개발하는 단계로, 사용자 요구사항을 구체화하는 단계이다.

SW개발보안 관점에서는 요구사항 분석에서 도출된 보안요구사항이 SW기능으로 구체화되는 단계이다. 구현시 SW개발보안가이드[9], 언어별 시큐어코딩 가이드[10,11] 등을 참조하면 보다 안전하게 구현할 수 있다.

개발자는 구현 단계를 통해 소스코드(및 소스코드 명세서)를 생성하고, 해당 문서에 최소한 다음과 같은 내용을 식별 및 기술해야 한다.

가. 보안요구사항이 포함되거나 중요한 기능을 구현한 소스코드 부분에 주석(및 소스코드 명세서에 별도 설명)으로 관련 내용 설명
나. 소스코드와 모듈간 매핑 관계
다. 소스코드에 대한 보안약점 분석 및 조치결과 등

개발자는 구현시 소스코드 보안약점 분석도구를 활용하여 소스코드에 존재할 수 있는 보안약점을 식별하여 제거하는 활동을 병행해야 한다. 현재 국내에서는 감리대상인 국가정보화사업을 통해 정보시스템 SW 개발시 보안약점을 식별하여 제거하는 보증활동이 의무화되어 있다.

2.4. 시험

시험은 사용자의 요구사항이 SW기능으로 정확하게 구현되었는지 단위모듈시험, 기능시험, 통합시험 등을 통해 확인하고, 기능 오류가 없는지 확인하는 단계이다.

SW개발보안 관점에서는 요구사항 분석에서 도출된 보안요구사항이 SW 기능에 반영되었는지 시험을 통해 확인하고, 취약점이 존재하지 않는지 확인하는 단계이다. 소스코드 정적분석을 통해 보안약점 존재 유무를, SW 기능 동작 기반의 동적분석을 통해 취약점 존재유무를 점검한다.

개발자는 시험 단계를 통해 시험서 및 취약점 분석서를 생성하고, 해당 문서에 최소한 다음과 같은 내용을 식별 및 기술해야 한다.

가. (시험서) 시험항목(모듈, 서브시스템, 기능, 보안기능) 및 SW 기능에 대한 시험 커버리지
나. (취약점분석서) SW 유형에 따른 공개된 취약점 항목 분석 및 적용 가능한 취약점 시험항목
다. (공통) 시험항목별 시험목적, 시험선행조건(시험도구, 설정 등), 시험절차 및 결과
라. (공통) 기능오류 및 취약점 발견에 따른 보완조치 이력
마. (취약점분석서) 잔여취약점 여부 등

2.5. 릴리즈(Release)

릴리즈는 SW 개발 완료시 진행되는 단계로, SW 배포하여 설치할 수 있도록 SW 배포본을 만드는 단계이다.

SW개발보안 관점에서는 개발자에 의해 수행된 보안약점 및 보안취약점 분석 활동 및 조치내역에 대해 최종 확인후 SW 배포본을 생성하는 단계이다.

개발자는 릴리즈 단계를 통해 SW 배포패키지와 SW 설치 및 운영설명서를 생성하고, 설치 및 운영설명서에 최소한 다음과 같은 내용을 식별 및 기술해야 한다.

가. SW 구성요소 및 기능
나. SW 설치 환경 및 설치방법, 설치 확인 사항 및 재구성 방법
다. SW 사용자별 권한 및 사용기능 구분
라. SW 설정 및 기능에 대한 설명
마. SW 기능 오류 및 대응방법 등

2.6. 유지보수

유지보수는 SW 운영 중 발생하는 기능 및 서비스 오류에 대한 조치를 수행하고, 개선이 필요한 기능을 구현 및 수정하는 단계이다.

SW개발보안 관점에서는 주기적으로 보안취약점을 점검하여 이에 대한 조치를 취하는 예방적인 성격을 가지는 단계이다.

SW 운영자는 연간 보안점검계획서를 생성하고, 계획서를 기반으로 보안점검 수행 및 조치한 결과를 생성해야 하며, 해당 문서에 최소한 다음과 같은 내용을 식별 및 기술해야 한다.

가. (계획서) 보안약점 및 보안취약점 점검 대상 및 주기, 점검방법(기준, 점검도구 등) 및 점검 수행자

나. (결과) 점검결과 및 조치내역 등

Ⅲ. 국내 SW 시험·인증 동향

개발자가 수행한 SW보증활동이 적절히 수행되었는지 시험 및 평가를 통해 확인하는 과정은 개발된 SW에 신뢰성을 부여하는 중요한 활동이다. SW보증수준에 따라 시험 및 평가의 수행범위는 다르며, SW 유형에 따라 시험 및 평가기준 또한 다르다. 국내에서 수행하고 있는 SW 시험인증 활동에 대해 설명한다.

3.1. 정보보호제품 평가·인증

정보보호제품 평가·인증은 정보보호제품이 평가기준에 부합하는지를 평가기관이 평가하고, 평가 결과를 인증기관이 승인하여 인증서를 발급하는 제도로, 국가정보화기본법 제38조 및 동법 시행령 제35조를 근간으로 하고 있다. 국내에서는 1999년 침입차단시스템에 대한 평가(K기준)를 시작으로, 침입탐지시스템에 대한 평가를 추가적으로 수행하였다. 2003년 국제평가규격인 공통평가기준(Common Criteria, CC)을 도입한 이후, 2006년 CC인증제품 수출 지원을 위해 국제상호인정협정(Common Criteria Recognition Arrangement, CCRA)에 인증서발급기관 자격으로 회원국으로 가입하였다. 현재, CC평가기관으로는 법적으로 정해진 KISA 이외에 (재)한국기계전기전자시험연구원(Korea Testing Certification, KTC)[12] 등 6개 기관이 평가기관으로 지정받았다. 평가기관 중 고등급(EAL5) 평가를 수행할 수 있는 기관은 국내에서 KTC 등 3개기관이 유일하다. 평가기관이 수행한 정보보호제품 평가결과를 승인하여 인증서를 발급해 주는 인증기관은 국가보안기술연구소 소속의 IT보안인증사무국에서 담당하고 있다.

〔그림 1〕 보증등급별 상세화 수준 및 시험·평가 범위[13]

CC평가·인증의 평가보증등급(Evaluation Assurance Level, EAL)은 평가신청기관이 제출한 보증문서를 기반으로 평가를 수행하여 부여되는 보증등급으로 EAL1부터 EAL7까지 있다. EAL 등급이 높아질수록 보증 요구사항이 증가하여 보증수준이 높아지게 된다. 일반적으로 EAL2는 제품을 구성하는 보안기능간의 상관관계에 대한 분석과 시험, EAL3 등급은 보안기능을 구성하는 하위 서브시스템에 대한 상관관계 분석과 시험, EAL4 등급은 서브시스템을 구성하는 하위 단위모듈에 대한 상관관계 분석과 시험을 요구한다[13]. 취약성 시험은 평가보증등급에 따른 공격자 수준을 기반으로 취약성 시험항목을 도출하여 수행한다.

따라서, 평가신청제품의 평가보증등급이 높을수록 보증요구사항 증가하고 수준도 높아지기 때문에 제품에 대한 분석 수준도 높아져서 제품에 대한 안전·신뢰성이 증가하게 된다.

현재, CC인증서의 통용범위에 따라 국내용과 국제용으로 CC평가인증이 이원화되어 운영되고 있으며, 국가·공공기관에 도입되는 정보보호제품 중 CC인증이 필수인 제품은 24종으로 평가보증등급은 EAL2 이상을 요구[14]하고 있다.

3.2. 신용카드 단말기 보안시험·인증

신용카드 단말기 보안시험은 최근 개정된 여신전문금융업법(법률 제13448호, 2015.7.2.) 제27조의 4에 따

〔그림 2〕 신용카드 단말기 보안 시험·인증 체계

라 신용카드회원의 정보보호를 위하여 금융위원회가 정하는 기술기준에 따라 신용카드 단말기의 보안기능의 안전성과 신뢰성에 대한 시험을 수행하여, 신용카드회원이 안심하고 제품을 사용할 수 있도록 지원하는 제도이다. 동법에 따르면, 2015년7월21일부터 가맹점에 신규 설치 및 교체되는 단말기가 민감한 신용카드 정보를 통해 거래가 이뤄지는 경우, 단말기의 형태와 상관없이 기술기준을 의무적으로 충족하여야 하며, 가맹점에서는 MS카드 불법복제 등의 사고를 예방하기 위해 신용판매 승인 시 IC카드를 우선적으로 적용해야 한다[15].

기술기준은 신용카드 단말기 유형(POS, CAT)에 따라 세부 보안기능 및 시험요구사항을 다음과 같이 제시하고 있으며, 시험은 기본 요구사항 및 기술적 요구사항에 대해 수행하고 있다. 관리적 요구사항은 신청업체가 제출한 제출문서를 통해 확인하고 있으며, 신용카드 단말기 제공업체 및 가맹점에서 관리 및 수행되도록 요구되고 있다.

〔표 1〕 신용카드 단말기 정보보호 기술기준〔16〕

구분	정보보호 요구사항
기본 요구사항	신용카드 거래승인(IC우선거래 등)
	신용카드 처리
기술적 요구사항	민감한 신용카드 정보보호(기밀성, 저장금지 등)
	신용카드 정보보호(전송·저장 보호 등)
	암호화(보안강도, 암호키 생성·분배 등)
	자체보호(무결성 점검 등)
관리적 요구사항	안전한 SW 개발
	초기 암호키 주입
	보안교육
	형상관리
	안전한 운영환경 구성
	보안취약점 점검 및 조치

현재 인증기관인 여신금융협회로부터 지정된 시험기관은 KTC 및 한국아이티평가원(KSEL)이 있으며, KTC의 경우, 여신금융협회의 인증업무 수행을 지원하고 있다.

3.3. SW 품질인증 및 프로세스 품질인증

SW 품질인증은 국제 표준(ISO/IEC TR 9126-2 / KS X ISO/IEC TR 9126-2, ISO/IEC 25051 / KS X ISO/IEC 25051)를 기반으로 신청기관이 제출한 SW 제품(Ready to Use Software Product, RUSP), 제품설명서, 시험서에 대한 각각의 품질에 대한 적합성 시험을 수행하는 것으로, GS(Good Software)인증으로 널리 알려져 있다. 미래창조과학부에서 시험인증기관을 지정하며, 현재 한국정보통신기술협회(TTA) 및 한국산업기술시험원(KTL)이 지정되어 있다.

SW 프로세스 품질인증은 SW 제품 자체보다는 SW 개발업체의 SW 개발 및 유지보수 프로세스에 대한 품질인증으로, 미래창조과학부에서 시험인증기관을 지정하며, 현재 정보통신산업진흥원(NIPA)가 지정되어 있다.

Ⅳ. 결 론

본 논문에서는 행정자치부 및 KISA의 SW 개발보안 활동을 통한 개발자 측면의 SW보증활동을 소개하였으며, 정보보호제품 평가·인증 및 신용카드 단말기 보안시험 제도 등 소개를 통해 SW보증과 관련된 국내 SW 시험·인증 동향에 대한 설명하였다.

국내 동향에 따르면, 현재 우리는 국가·공공기관 도입 요건과 법적인 요구조건을 통해 SW 개발사들에게 SW 보증을 요구하고 있으며, SW 판매를 위해 SW 개발사들이 제품개발완료 이후 끼워 맞추다시피 SW보증 활동을 역으로 하고 있다.

따라서, 국내 SW의 품질 및 보안성 제고를 통한 국내외 경쟁력 향상을 위해서는 SW개발업체가 자발적으로 SW 보증활동을 수행할 수 있는 환경 제공이 필요하며, 이를 지원하는 다양한 가이드 개발·보급과 교육이 수반되는 것이 필요하다.

참 고 문 헌

[1] Software & Supply Chain Assurance, https://buildsecurityin.us-cert.gov/swa

[2] 행정안전부, “정보시스템 구축·운영 지침”, 행정안전부고시 제2012-25호, June 2012.

[3] Microsoft, Inc., Benefits of the SDL : More Secure Software, http://www.microsoft.com/security/sdl/learn/measurable.aspx

[4] OWASP, OWASP CLASP Project, https://www.owasp.org/index.php/CLASP

[5] G. McGraw, *Software Security : Building Security In*, Addison Wesley, 2006.

[6] 방지호, 하란, “전자정부 소프트웨어의 보안약점 진단도구 평가방법론”, *한국통신학회논문지*, Vol.38C No.04, pp.335-343, April 2013.

[7] Software engineering Institute, “Secure Design Patterns”, TECHNICAL REPORT CMU/SEI-2009-TR-010, 2009.

[8] J.Y. Dangler, “Categorization of Security Design Patterns”, East Tennessee State University, May 2013.

[9] 행정자치부, “소프트웨어 개발보안 가이드”, 행정자치부·KISA, November 2013.

[10] 행정자치부, “JAVA/C/Android JAVA 시큐어코딩 가이드”, 행정자치부·KISA, September 2012.

[11] SEI CERT Coding Standards https://www.securecoding.cert.org/confluence/display/seccode/SEI+CERT+Coding+Standards

[12] (재)한국기계전기전자시험연구원, http://www.ktc.re.kr, http://ict.ktc.re.kr

[13] 이강석, 임재명, 방지호, “정보보호제품 평가의 보증등급과 보안기능강도와의 상관관계 분석”, 한국통신학회 종합 학술 발표회 논문집(하계) 2009, pp.1627-1628, June 2009.

[15] IT보안인증사무국, http://www.itscc.or.kr

[16] 여신금융협회, https://www.crefia.or.kr

[17] 여신금융협회, “신용카드 단말기 정보보호 기술기준”, April 2015.

〈저 자 소 개〉

방 지 호 (BANG JI HO)
정회원

1997년 2월 : 홍익대학교 컴퓨터공학과 졸업
2001년 8월 : 홍익대학교 컴퓨터공학과 석사
2014년 2월 : 홍익대학교 컴퓨터공학과(정보보호) 박사
2001년 7월~2014년 8월 : 한국인터넷진흥원(구 한국정보보호진흥원) 책임연구원
2014년 9월~현재 : (재)한국기계전기전자시험연구원 선임연구원
관심분야 : 모바일/SW보증, IoT 보안, 클라우드 컴퓨팅

지 재 덕 (JI JAE DEOK)
정회원

1996년 2월 : 고려대학교 금속공학과 졸업
1998년 2월 : 고려대학교 금속공학과 석사
2012년 8월 : 고려대학교 정보보호대학원 박사
2007년 1월~2011년 10월 : 한국인터넷진흥원(구 한국정보보호진흥원) 책임연구원
2011년 11월~현재 : (재)한국기계전기전자시험연구원 정보보안평가센터 센터장
관심분야 : 부채널, 오류주입 공격, IoT 정보보호기술