

# 보안용 소프트웨어 기능성과 일반적 요구사항의 시험사례 분석<sup>+</sup>

강배근\* ,이하용\*\*, 양해술\*\*\*

\*호서대학교 혁신기술경영융합대학원, \*\*서울벤처정보대학원대학교,

\*\*\*호서대학교 벤처전문대학원

e-mail : dandyishkang@gmail.com, lhyazby@suv.ac.kr, hsyang@office.hoseo.ac.kr

## Software ability for security and examination example analysis of general requirement

Bae-Keun, Kang\*, Ha-Yong Lee\*\*, Hae-Sool Yang\*\*\*

\*Graduate School of Multidisciplinary Technology and Management, Hoseo Univ.

\*\*Seoul Univ. of venture & information,

\*\*\*Graduate School of Venture, Hoseo Univ.

### 요 약

최근 보안용 소프트웨어에 대한 결합사항이 증대됨에 따라, 관련 서비스 즉, 보안용 소프트웨어 품질을 평가하고 개선하기 위한 기술이 집중적으로 요구되며 품질평가 방안에 대한 연구와 시험기술 개발이 요구된다. 따라서 본 연구에서는 보안용 소프트웨어의 기능성과 일반적 요구사항의 시험 인증 사례를 통해 수집데이터를 근거로 필수적으로 확보해야 할 품질 수준을 정의하고 품질수준을 도출과 결합의 유형 분석을 통하여 기능성 개발단계 상의 취약부분을 도출함으로써 품질향상을 최적화하고자 한다.

### 1. 서 론

최근 보안용 소프트웨어에 대한 결합사항이 증대됨에 따라, 관련 서비스 요구사항을 충족시키고, 품질향상을 실현을 위해서는 시험 및 품질에 대한 컨설팅이 지속되고 있다. 또한, 보안용 소프트웨어 품질을 평가하고 개선하기 위한 기술이 집중적으로 요구되며 품질평가 방안에 대한 연구와 시험기술 개발이 요구된다.

따라서 본 연구에서는 보안용 소프트웨어의 기능성과 일반적 요구사항의 시험 인증 사례를 통해 수집데이터를 근거로 필수적으로 확보해야 할 품질 수준을 정의하고 품질수준을 도출과 결합의 유형(도큐먼트 결합, 과부하 결합 등) 분석으로 기능성 개발단계 상의 취약부분을 도출함으로써 품질향상을 최적화하고자 한다.

본 연구의 구성은 아래와 같다. 먼저 2장에서는 보안용 소프트웨어의 관련연구에 대해 기술하였고 3장에서는 ISO/IEC 12119를 기반으로 하여 보안용 소프트웨어의 기능성에 대한 시험모듈을 제시하였으며 4장에서는 시험환경 구축을 기술하였으며 5장과 6장에서는 보안용 소프트웨어의 기능성과 일반적 요구사항을 제안된 매트릭을 중심으로 시험 결과서를 작성하고 분석하였다. 마지막으로 7장에서는 결론과 향후 과제를 기술하였다.

### 2. 관련 연구

#### 2.1 ISO/IEC 9126과 ISO/IEC 12119의 체계

본 시험은 ISO/IEC 9126과 ISO/IEC 12119에 근거하여 개발된 품질 평가 모형을 기준으로 측정하였으며 각각의 품질특성으로는 소프트웨어가 특정 조건에서 사용될 때, 명시된 요구와 내재된 요구를 만족하는 기능을 제공하는 기능성과 성능 수준을 유지할 수 있는 신뢰성, 사용자가 이해하고, 학습하며, 사용하고 선호할 수 있는 사용성, 자원의 양에 따라 요구된 성능을 제공하는 효율성, 소프트웨어 제품이 변경되는 능력을 의미하며, 변경에는 환경과 요구사항 및 기능적 명세에 따른 소프트웨어의 수정, 개선, 또는 개작 등이 포함된 유지보수성, 특정한 환경에서 다른 환경으로 전이될 수 있는 소프트웨어 제품의 능력인 이식성과 마지막으로 제품 정보 제공 능력 및 제품의 바이러스 감염 여부를 나타내는 일반적 요구사항이 있다.

#### 2.2 정보보호 시스템 평가 제도

##### 2.2.1 평가제도 시행 배경

컴퓨터와 통신기술이 결합한 정보통신의 비약적인 발전에 따른 정보화의 가속화는 필요한 정보제공 서비스 등으로 유익한 정보를 공유할 수 있는 혜택을 주는 반면, 개인 및 국가 사회의 중요한 정보가 각종 정보통신망을 통한 불법적 침입, 공격 등 날로 증가되는 위협에 직면하고 있다. 이에 대응한 네트워크 보안 대책으로써 정보보호시스

<sup>+</sup> 본 연구는 지식경제부와 IITA의 대학 IT연구센터 지원사업의 연구결과로 수행되었음(IITA-2009-(C1090-0902-0032)).

템의 사용이 점차 증가하는 추세에 있으며 현재 국내에서는 이러한 추세에 따라 국내외에서 개발한 많은 종류의 정보보호시스템이 공급되고 있으며 기업 및 공공 전산망에서 침입차단시스템과 침입탐지시스템 등의 도입요구가 급증하고 있다.

그러나 보안기능의 성능과 신뢰도가 증명되지 않은 시스템의 사용은 보안 취약성이 내재되어 있을 가능성이 있으므로 이를 해결하기 위한 방안으로 정부에서는 정보통신망 침입차단시스템과 침입탐지시스템의 평가기준 및 평가지침서를 고시하였으며 한국정보보호진흥원에서 침입차단시스템 평가제도를 도입하여, 침입탐지시스템 평가를 시행하고 있다.

2.2.2 정보보호 시스템 평가 목적

정보보호 시스템 평가 목적으로는 보안기능에 대한 성능 및 신뢰도가 검증된 정보보호시스템 보급을 촉진하고 평가대상 제품을 평가기준 및 평가지침서의 평가 등급별 요구사항을 근거로 평가하여 제품에 구현되어 있는 보안기능의 신뢰성을 보증함으로써 개인과 기업 및 공공 기관에서 안심하고 평가 인증 받은 신뢰된 제품을 사용할 수 있는 여건을 조성하며 안전한 정보보호시스템 공급에 의한 정보화를 촉진할 수 있다.

2.2.3 정보보호 시스템 기대효과

정보보호 시스템 기대효과로는 정보보호산업 육성 기반을 조성하고 정보보호기술 및 정보보호제품에 대한 민간 및 공공 기관의 인식을 확산시켜 정보보호의 필요성에 대한 공감대를 형성하는 효과를 불러일으킴으로써 정보보호 제품 시장을 활성화하며 정보보호산업체의 정보보호 기술력 향상 유도하고 평가기준 및 평가지침서를 제시하여 정보보호기술의 지침을 제시하고 평가 수행을 통하여 정보보호시스템의 취약한 부분을 발견 및 개선하도록 유도하며 정보보호평가 및 개발 기술을 축적하여 정보보호산업체의 정보보호기술력 향상을 유도할 수 있을 것이다.

3. 보안용 소프트웨어의 기능성 시험모듈

보안용 소프트웨어는 사용자 본인 확인을 하는 인증 프로그램이나 데이터베이스에 접근하는 사용자와 응용 프로그램의 접근통제를 수행하는 데이터베이스 보안 프로그램, 데이터베이스에 저장되는 데이터를 암호화하거나 복호화하는 등의 기능을 수행하는 소프트웨어 분야이며 주로 많은 결함이 나타나는 기능성의 시험모듈은 아래와 같다.

3.1 기능성 시험 모듈

소프트웨어 제품이 제한 받고 있는 경계값의 범위를 벗어난 입력에 대한 예외처리를 하고 있는가를 측정하는 경

계값 처리율의 시험모듈이며 측정항목은 사용자 문서에 명세된 경계값에 대한 테스트케이스를 작성하는 '경계값 확인 대상 항목 수'와 테스트케이스에 따라 테스트를 수행하여 명세와 일치하는 경우를 체크하는 '각 항목별 테스트 케이스 성공률의 합'으로써 계산식으로는 <표 1>과 같다.

<표 1> 경계값 처리율 계산식

부특성	기능성		
계산식	- 경계값 처리율 = B/A $B = \frac{\sum_{i=1}^A \text{Success\_TC}_i}{\text{Total\_TC}_i}$		
	- Success_TC : i 번째 경계값 처리 기능 확인을 위해 수행한 테스트 케이스 중 성공한 건 수 - Total_TC : i 번째 경계값 처리 기능 확인을 위해 수행한 테스트케이스 수		
결과영역	0 ≤ 경계값 처리율 ≤ 1	적용대상	공통

프로그램이 사용자 문서에 기술되어 있는대로 정확하게 구현되는지를 측정하는 기능구현 정확성의 시험모듈이며 측정항목은 '평가되어야 하는 기능의 수'와 '각 항목별 테스트케이스 성공률의 합'으로써 계산식으로는 <표 2>와 같다.

<표 2> 기능 구현 정확성 계산식

부특성	기능성		
계산식	- 기능구현 정확성 = B/A $B = \frac{\sum_{i=1}^A \text{Success\_TC}_i}{\text{Total\_TC}_i}$		
	- Success_TC : i 번째 기능 확인을 위해 수행한 테스트케이스 중 성공한 건 수 - Total_TC : i 번째 기능 확인을 위해 수행한 테스트케이스 수		
결과영역	0 ≤ 기능구현 정확성 ≤ 1	적용대상	공통

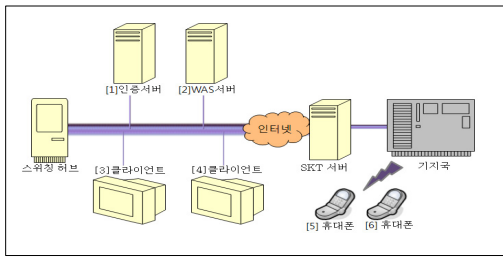
4. 보안용 소프트웨어의 시험

이 절에서는 보안용 소프트웨어를 시험하기 위해 필요한 시험 환경에 대해 기술하고자 한다. 먼저, 보안용 소프트웨어 시험을 위한 절차와 시험환경에 대해 살펴보기로 한다.

4.1 시험 절차

시험 절차로는 먼저 시험을 하고자 하는 제품의 시험계획을 수립하고 시험 환경을 구축하여 시험 환경을 구성할 수 있도록 하고 제안한 메트릭에 대하여 시험 항목을 도출하며 테스트 시나리오와 케이스를 작성하고 시험을 수행한다. 시험 도중 발생하는 결함에 대해서는 결함리포트를 작성하고 결함리스트를 중심으로 하여 제품의 패치를 통해서 결함을 수정하고 다시 제품에 대한 회귀시험을 수행하여 시험결과를 작성한다.

4.2 시험환경 구축



(그림 1) 보안용 소프트웨어 시험 절차

(그림 1)과 같이 시험환경을 구축하였으며 [1]번 서버에 설치한 프로그램으로는 시험 대상 제품(인증 서버 모듈)을 사용, [2]번 서버에 설치한 프로그램 시험 대상 제품(웹애플리케이션 모듈), 샘플 웹애플리케이션으로는 WAS: Apache Tomcat 6.0, DBMS: Mysql 4.1.7, JDK 1.6이 사용되었으며 [3], [4]번 클라이언트에 설치한 프로그램으로는 Microsoft Internet Explorer 6.0, 일반 응용프로그램: MS-Office 2002, 한글 2005, 바이오봇 Desktop 5.5 등이 설치되었고 [5], [6]번 휴대폰에 설치한 프로그램으로는 시험 대상 제품(1회용 패스워드 생성 모듈), 네트워크로는 10/100Mbps 스위칭 허브를 사용하였다.

성능측정도구로는 TeamQuest v10.1(서버 자원 사용률 측정)이 사용되었고 [1]번 서버에 TeamQuest v10.1 Manager를 설치, [3]번 클라이언트에 TeamQuest v10.1 View를 설치하였고 [1]번 서버에 가상의 휴대폰 사용자를 생성하는 시뮬레이터를 설치하여 측정하였다.

5. 기능성과 일반적요구사항의 시험 결과

본 제품은 휴대폰에서 생성한 1회용 패스워드를 웹사이트에 입력함으로써 사용자 본인임을 확인해주는 사용자 인증 프로그램으로 주요 기능으로는 사용자 정보 관리, 등록코드 발급, 1회용 패스워드 생성(보안카드 타입, 패스워드 변경 타입), 사용자 인증이 있다.

보안용 소프트웨어의 기능성과 일반적 요구사항을 제안된 메트릭을 중심으로 시험 결과서를 작성하였고 기능성과 일반적 요구사항의 최종결합수의 집계표는 <표 2>와 같다.

<표 2> 시험 전/후의 결합수

품질특성	수정전 결합수	최종 결합수
기능성	4	0
일반적 요구사항	4	0
계	8	0

6. 기능성과 일반적 요구사항의 결합 분석

6.1 결합 내역

품질특성 및 결합속성별로 기능성과 일반적 요구사항에 대한 사례를 분석한 결합 건수 및 내역 등을 정리하면 <표 3>와 같다.

<표 3> 결합 내역

품질특성	결합수	결합정도	결합요약	최종결합사항
기능성	4	H	모바일 모듈프로세스 시작 오류	0
		H	인증 기능오류	
		M	1회용패스워드생성 오류	
		H	대량 인증기능 오류	
일반적 요구사항	4	M	제품 식별 정보 미제공	0
		M	제품 공급자정보 미제공	
		M	제품지원 정보 미제공	
		M	제품인도항목정보 미제공	
합계	8			0

6.2 결합속성 분석

보안용 소프트웨어의 기능성과 일반적 요구사항의 결합을 분석한 결과는 다음과 같다.

6.2.1 기능성

보안용 소프트웨어의 기능성 결합은 제공된 기능이 정상적으로 동작하지 못하는 기능오류가 총 4건중 전체를 차지하고 있으며 결합속성을 살펴보면 인증기능 오류나 1회용 패스워드생성 오류와 같이 제공되는 기능에 결합이 나타나는 경우가 많은 것을 알 수 있었으며 수정 보완 및 회귀시험 과정을 거친 후 최종적으로 정상 동작함을 확인하였다.

6.2.2 일반적 요구사항

보안용 소프트웨어의 일반적 요구사항의 결합으로는 구현된 기능에 대한 정보가 제공되지 않는 경우가 다수 나타나고 있음을 알 수 있었으며 수정 보완 및 회귀시험 과정을 거친 후 최종적으로 정상 동작함을 확인하였다.

6.3 보안용 소프트웨어의 시험 관련사항

6.3.1 결합 정도 분석

결합 정도의 분류는 H(High)인 경우 기능이 정상적으로 동작하지 않거나, 시스템(하드웨어) 혹은 프로그램이 비정상적으로 종료되는 등의 치명적인 결합이 발생하는 경우로 분류하며 M(Medium)은 프로그램 운영에는 문제가 없으나, 기능이 정확하게 동작하지 않거나 사용자의 혼란을 야기하는 정도의 결합이 발생하는 경우로 분류할 수 있으며 L(Low)은 프로그램 운영에 문제가 없고, 기능도

정확하게 동작하나 권고 사항 수준의 경미한 결함이 발생하는 경우를 들 수 있다.

결함정도 분포에 따르면 기능성의 결함은 기능이 정상적으로 동작하지 않거나 인증하는데 오류가 발생하는등의 치명적인 결함이 발생하는 경우인 High가 총 4건 중 3건을 차지하였으나 수정 보완 및 회귀시험 과정을 거친 후 최종적으로 정상 동작함을 확인하였다. 일반적 요구사항의 결함은 프로그램 운영에는 문제가 없으나, 기능이 정확하게 동작하지 않거나 사용자의 혼란을 야기하는 정도의 결함이 발생하는 경우인 M(Medium)이 총 4건의 결함 중 전체를 차지하였으며 수정 보완 및 회귀시험 과정을 거친 후 최종적으로 정상 동작함을 확인하였다.

컴퓨터·소프트웨어 기술연구소 위탁과제 최종보고서, 2001. 11.

## 7. 결 론

본 연구에서는 ISO/IEC 12119를 기반으로 하여 보안용 소프트웨어의 평가 모델을 개발하고 평가 과정에서 활용할 수 있는 기능성을 측정할수 있는 품질검사표를 개발하였다. 또한, 보안용 소프트웨어의 기능성과 일반적 요구사항에 대한 시험평가 방법을 구축하여 품질 수준 제고와 대외 경쟁력을 향상시키기 위한 연구를 수행하였다.

보안용 소프트웨어의 기능성과 일반적 요구사항의 평가 모델 개발과 향후 실질적인 활용을 통해 고품질 보안용 소프트웨어의 개발을 촉진함으로써 국제적으로 경쟁력을 갖춘 보안용 제품의 개발을 지원할 수 있을 것으로 기대한다.

## 참고문헌

- [1] K. Romer, T. Schoch, F. Mattern and Dubendorfer, "Smart Identification Frameworks for Ubiquitous Computing Applications", Proceedings of the First IEEE International Conference on Pervasive Computing and Communications, pp.256-262, 2003.
- [2] Moller, K.H. and Paulish, D.J., "Software Metrics", Chapman & Hall(IEEE Press), 1993.
- [3] ISO/IEC 12119:1994, Software Engineering - Software product evaluation - Requirements for quality of commercial -off -the -shelf software products (COTS) and instructions for testing.
- [4] ISO/IEC 13407:1999, Human-centered design processes for interactive systems.
- [5] 양해술, 정혜정, 이하용, "의료용 소프트웨어의 평가기준 개발", 식품의약품안전청, 최종보고서, 2002.
- [6] 한국정보통신기술협회, "품질메뉴얼/ 공통품질절차서/ 시험품질절차서/인증품질절차서, TTA 소프트웨어시험인증센터.
- [7] 한국정보통신기술협회, "소프트웨어 테스트 전문기술", 응용과정편, TTA, 소프트웨어시험인증센터, 2006.
- [8] 양해술, "소프트웨어 시험평가 모듈 개선 연구", ETRI