보안소프트웨어 제품을 위한 평가 매트릭스 연구

이종민°
고려대학교 정보통신대학 컴퓨터 정보통신대학원 소프트웨어공학과
chlish°@korea.ac.kr

Investigation in Evaluation Matrix for Security Software Product

Jongmin Lee°
Dpt. Software Engineering, Graduate of School Computer and Information Technology,
College of Information and Communications, Korea University.

요 약

소프트웨어의 다양화로 인하여 하드웨어 형태의 보안 제품에서 소프트웨어 형 보안 제품으로 점차 변화하고 있는 중이다. 이러한 변화 속에서 소프트웨어 형 보안 제품의 품질을 평가하는 기준이 없어, 현재 ISO/IEC 9126 의 표준으로 소프트웨어 형 보안 제품을 평가하고 있는 것이 현실이다. 하지만 소프트웨어 형 보안 제품을, 기존 소프트웨어 품질 평가 기준으로 적용하기에는 한계가 있다. 지금까지 소프트웨어 제품의 평가 방법과 요구 사항에 대한 프로세스가 국제 표준으로 제정 및 정의되어 있으나, 소프트웨어 형 보안 제품의 경우, 이러한 국제 표준을 적용하여 제품을 평가하는 데는 어려움이 있다. 이에 본 논문에서는 현재 사용중인 소프트웨어 평가 기준 인ISO/IEC 9126-1에서 규정하고 있는 6개의 소프트웨어 품질특성 중 기능성 의 부 특성인 보안성의 매트릭스를 확인하고 ISO/IEC 15408(공통평가기준)의 내용 중 일부를 발췌 및 보완하여 기존 6가지의 소프트웨어 품질특성 중 기능성의 부특성인 보안성을 보완한, 새로운 보안성 품질 매트릭스를 제안한다.

1. 서 론

소프트웨어 제품의 품질은 소프트웨어의 사용이 광범위 해지기 시작 하면서 가장 큰 관심사항으로 되었다. 이러한 이유로 국내 및 세계 여러 나라들이 소프트웨어 품질 평가 및 인증제도를 시행하고 있다[13]

하지만 소프트웨어의 종류가 다양해지고, 제품형태에 따라서 요구사항 및 제품의 수준이 차별화 되어, 소프트웨어 제품을 평가한다는 것은 쉽지 않은 실정이다.

이러한 소프트웨어 제품의 평가를 위하여, 국내외 많은 기관 및 연구소에서 품질에 대한 방법 과 방법론을 연구하고 있으며, 대체로 국제표준 ISO/IEC 9126의 소프트웨어 품질 평가 매트릭스를 기준으로 하고 있다. 이러한 평가 매트릭스는 환경적인 여건이나 기타 국내의 실정에 반영되기 힘든 평가 항목들이 다소 있으며, 이러한 개선방안을 연구 해야 하는 문제점등이 발생을 했다.

현재 국제 표준 기구 ISO/IEC, JTC1/SC&/WG6에서는 소프트웨어 품질 평가 표준인 ISO/IEC 9126 과 ISO/IEC 14598의 평가 매트릭스를 다시 정리하여 SQuaRE(Software product Quality Requirements and Evaluation) 라는 새로운 매트릭스를 개발하여,제품의 품질 평가 표준을 만들기 위한 연구를 진행중에 있고, 국내에서도 적극적으로 참여 하여 국내의 소프트웨어 품질 평가를 위한 표준을 제정하기 위한 노력을 하고 있다.[14]

ISO/IEC 9126 에서는 소프트웨어 품질 평가를 위한 매트릭스는 기능성(Functionality),신뢰성 (Reliability), 사용성 (Usability), 유지보수성(Maintainability), 효율성(Efficiency),이식성(Portability) 등 6가지 품질 특성으로 나누어 평가 되어 지고 있으며, 이러한 평가 기준에 의해서 부수적인 평가 항목들로 구성되어 있다.

하지만 시대가 지날수록 하드웨어와 소프트웨어의 경계가 사라지고, 기존의 하드웨어 형태의 보안 제품이 소프트웨어 형태로 변하고 있는 상황에서, ISO/IEC 9126 의 평가 모델로 소프트웨어 형 보안 제품을 평가 하기에는 요구 사항이 명확하지 않는 문제가 발생되었다.

ISO/IEC 9126의 세부매트릭스 중 기능성의 부 특성으로 보안성을 평가하고 있지만, 평가기준이 범위가 작고, 보안 기능의 일부분에 대한 평가 기준 이여서 소프트웨어 형 보안 제품으로 평가하는 기준으로 사용되기에는 부적절 하다. 또한 보안 제품의 경우 이미 한국정보보호진흥원에서 ISO/IEC 15408 공통평가 기준 (CC: Common Criteria)으로 보안제품의 평가 하고 있다.

본 논문에서는 현재 적용되고 있는 ISO/IEC 9126 과 ISO/IEC 14598의 통합 표준인 SQuaRE에 대한 설명과 ISO/IEC 9126 의 평가 매트릭스를 가지고 소프트웨어 형 보안 제품의 평가에 대한 문제점을 기술 하였고, 제2장 본론에서는 소프트웨어 품질 평가(ISO/IEC 9126)의 품질 특성 매트릭스 와 ISO/IEC 15408에 대한 평가 매트릭스에 대하여 설명할 것이다. 제3장에서는 새로운 평가 시험항목을 제시할것이며,제4장에서 새로운 평가모델에 대한 검증을 할 것이며, 마지막으로 제5장에서는 향후 연구 방향과 결론을 논의하겠다.

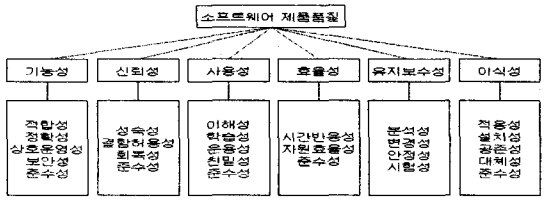
2. 본론

본 장에서는 소프트웨어 품질평가 와 보안성 평가매트릭스에 대하여 분석하겠으며, 보안제품의 평가 모델인 ISO/IEC 15408 공통평가기준 에서 보안제품의 평가 세부 매트릭스를 추출하겠다.

2.1 소프트웨어 품질평가 (ISO/IEC 9126)

소프트웨어의 품질은 소프트웨어의 기능과 성능,만족도에 있어서 명시된 요구사항 및 내제된 요구사항을 얼마나 충족하는가를 나타내는 소프트웨어의 총체이다. 따라서 소프트웨어 제품의 품질은 소프트웨어 제품 특성에 따른 다양한 요구사항을 충족시킴으로써 확립된다. ISO/IEC 9126은 소프트웨어 품질모델을 규정하는 국제표준으로, 소프트웨어의 품질을 확립하고, 평가하는데 중요한 지침이 된다. 지난 2000년에 개정된 ISO/IEC 9126-

1 에 따르면, 품질 평가의 핵심인 소프트웨어 품질 특성과 부 특성은 <그림 1>와 같다.[1]



<그림 1 소프트웨어 품질특성 과 부 특성>

<그림1>과 같이 제시된 품질특성은 다수의 매트릭스를 통해 수행된다. 이와 같은 국제 표준들은 포괄적이고 추상적인 부분들이 많이 때문에, 특정 국가에 표준을 적용하기 위해서 국제표준을 중심으로 자국 실정에 맞는 국가별 표준을 제정하고 사용하고 있다. 우리나라에도 자국의 실정에 맞게 ISO/IEC 9126-1을 토대로 개발 되었다. 현재 한국정보통신 기술협회에서 사용되고 있는 국내 시험 항목은 <표1> 과 같다. [2]

대항목	소항목
일반적 요구사항	식별 및 표시
기능성	적합성,정확성,상호 운영성,보안성,준수성
신뢰성	성숙성,오류 허용성,회복성,준수성
사용성	이해가능성,학습성,운영성,선호도,준수성
효율성	시간효율성,자원효율성,준수성
유지보수성	분석성,변경성,안정성,시험가능성,준수성
이식성	적응성,설치가능성,대체성,공존성,준수성

<표1.소프트웨어 품질평가를 위한 시험항목>

2.2 보안성 (Security)

보안성은 ISO/IEC 9126 에서 정의한 품질 평가 매트릭스중 기능성의 하위 부특성이다.

기능성(Functionality)은 소프트웨어가 특정조건에서 사용되어질 때 명시된 요구 와 내재된 요구를 만족하는 기능을 제공하는 소프트웨어 제품의 능력을 의미 하는것으로 소프트웨어가 무엇을 하는가를 평가하는 것으로 적합성, 정확성, 상호운영성,보안성,준수성의 부특성으로 구성되어 있다. 보안성(Security)는 권한이 없는 사람이나 시스템은 정보를 읽거나 변경하지 못하게 하고 권한이 있는 사람이나 시스템은 정보에 대한 접근이 가능하도록 정보를 보호 하는 소프트웨어 제품의 능력을 의미 한다

2.3 보안성 평가 세부 매트릭스

보안성 평가에 대한 세부 매트릭스는 크게 4가지의 세부 기능에 대한 점검표를 가시고 있다. 첫번째는 접근통제 정보 제공 이며, 두번째는 접근통제 가능성, 세번째는 접근 감시 정보 제공, 마지막으로 접근 감시 가능성 에 대하여 평가를 한다. [3],[4]

2.3.1 접근통제 정보 제공

권한이 없는 사용자의 불법적인 접근을 통제하는 기능에 대한 정보 제공 여부를 의미한다. 평가 방법으로는 제품설명서와 사용자 문서에 보안과 관련된 접근통제 기능에 대한 정보가 기술되어 있는지 평가를 한다. 측정 방법은 <표2> 와 같은 항목으로 평가 한다.

측정항목	평가대상	측정유형
접근통제에 대한 정보의 제공 여부 (A)	D	Y/N/NA

<표2. 보안성-접근통제 정보제공 항목>

세부평가방법으로는 다음과 같다.

A: 접근통제에 대한 정보의 제공

(1)소프트웨어 제품의 사용권한이 있는 사람의 엑세스 허용

(2)소프트웨어 제품이 권한이 없는 사람 혹은 시스템은 정보에 대한 엑세스를 거부

(3) 사용자에 따라 선택적으로 사용권한 부여 가능

(4) 데이터의 복제를 방지하기 위한 기능

2.3.2 접근통제 가능성

허가 받지 않은 불법 사용자에 대한 접근통제 기능의 구현 여부를 의미한다. 평가 방법으로는 제품 설명서와 사용자 문서에 기술되어 있는 보안과 관련된 접근 통제 기능이 프로그램에 구현되어 있는지 평가한다. 측정방법은 <표3>과 같은 항목으로 평가 한다.

측정항목	평가대상	측정유형
접근통제를 위한 모든 기능 수 (A)	D,P	Number
각 항목별 테스트케이스 성공율의 합 (B)	P	Nimber

<표3. 보안성-접근통제 가능성 항목>

세부평가방법으로는 다음과 같다.

A: 접근통제를 위한 모든 기능 수

(1) 소프트웨어 제품의 사용권한이 있는 사람의 엑세스 허용

(2) 소프트웨어 제품이 권한이 없는 사람 혹은 시스템은 정보에 대한 엑세스를 거부

(3) 사용자에 따라 선택적으로 사용권한 부여 가능

(4) 데이터의 복제를 방지하기 위한 기능 등.

B: 각 항목별 테스트 케이스 성공률의 합

(1) 접근통제 기능에 대한 테스트 케이스를 시험하여 성공한 경우를 선택

2.3.3 접근 감시 정보 제공

사용자의 접근에 대한 제반 내역을 작성함으로써 감시 기능을 제대로 수행하는가를 의미한다. 평가 방법으로는 제품설명서와 사용자 문서에 보안과 관련된 정보중 접근 감시에 대한 정보가 기술되어 있는지를 평가 한다. 측정방법은 <표4>와 같은 항목으로 평가한다.

측정항목	평가대상	측정유형
접근 감시에 대한 정보의 제공 여부(A)	D	Y/N/NA

<표4. 보안성-접근 감시 정보 제공 항목>

세부평가방법으로는 다음과 같다.

A: 접근감시에 대한 정보의 제공 여부

(1) 소프트웨어 제품이 권한이 없는 사람 혹은 시스템은 정보에 대한 엑세스를 거부 해야 하며, 그 결과를 로그 파일로 작성하는 기능

(2) 사용자가 수행하는 작업을 로그파일로 작성하는 기능

(3) 접속한 사용자에 대한 로그파일 작성 기능 등. 이 있다.

2.3.4 접근 감시 기능성

접근 감시 기능이 명세된 대로 동작하는가에 대한 속성이다. 평가 방법으로는 제품설명서와 사용자 문서에 기술된 대로 프로그램의 접근 감시 기능이 동작하는지 평가 한다.

측정 방법은 <표5> 와 같은 항목으로 평가한다.

측정항목	평가대상	측정유형
접근감시에 이용되는 모든 기능의 수(A)	D,P	Number
각 항목별 테스트케이스 성공율의 합 (B)	P	Number

<표5.보안성-접근감시기능성 항목>

세부평가 방법으로는 다음과 같다.

A: 접근 감시에 이용되는 모든 기능의 수

(1) 소프트웨어 제품이 권한이 없는 사람 혹은 시스템은 정보에 대한 엑세스를 거부해야 하며, 그 결과를 로그 파일로 작성 하는 기능

(2) 사용자가 수행하는 작업을 로그 파일로 작성하는 기능

(3) 접속한 사용자에 대한 로그 파일 작성 기능 등.

B: 각 항목별 테스트케이스 성공률의 합
(1) 접근 감시 기능에 대한 테스트 케이스를 시험하여 성공한 경우를 체크 등이 있다.

2.4. 공통평가 기준(Common Criteria :CC)
2.4.1 국내 평가.인증 제도와 공통 평가 기준
2.4.1.1 국내 평가 인증 제도
국내 정보보호시스템 평가 인증제도는 정보화촉진법 및 동법 시행령에 의거 1998년 2월 정보통신망 침입차단시스템 평가기준(정보통신부고시 1998-19) 및 평가지침서 (정보통신부 고시 1998-20)가 고시되면서 시작되었으며, 이후 개정된 침입차단 시스템 평가기준(정보통신부 고시 2000-14)과 정보통신망 평가 인증지침(정보통신부 고시 2000-15)이 2000년 2월에 고시됨으로써 정보보호 산업체는 공공기관용과 민수용의 구분이 없는 단일 평가 인증체계 하에서 제품의 평가 인증 서비스가 시작되었다. 또한 국내 정보보호 시장의 침입차단시스템에 이어 추가로 침입탐지시스템이 평가 인증 대상에 포함됨으로써(정보통신부 고시 2000-62,정보통신부 고시 2000-24) 국내 정보보호 산업이 정착할 수 있는 기회가 되었다.[5][9]
2002년에는 한국정보보호 진흥원 및 국내 관계기관이 평가 인증제도의 국제적인 추세인 CC 버전 2.1을 국내 평가 기준으로 수용한 정보보호 시스템 공통평가기준(정보통신부 고시 2002-40)과 이를 시행하기 위한 정보보호 시스템 평가인증지침을 2002년 8월에 개정 고시 (정보통신부 고시 2002-41)하였다. [7],[8]
2.4.1.2 공통평가기준 (CC: Common Criteria for Information Technology Security Evaluation)
공통평가 기준은 1980년대부터 시행된 국가별 상이한 평가기준을 단일한 평가기준으로 대처하기 위하여 개발되었다. 현존하는 평가기준의 조화를 통하여 평가결과의 상호인증(Mutual Recognition)추진과 보안 요구사항의 유연성 부여, 평가의 상호인증을 위한 골격제시, 평가 기준의 향후 발전방향 정립을 목적으로 개발되었다.[6]
가. 공통평가기준 구조
공통평가기준은 크게 3부분으로 구성되어 있다.
Part 1 에서는 소개 및 일반모델을 제시하고 있으며 Part 2 는 보안기능 요구사항, Part·3 은 보증 요구사항을 포함하고 있다. CC 의 핵심은 Part 2 와 Part 3 으로 정보보호시스템이 구비해야 하는 기능 및 보증 요구사항을 기술하고 있으며 개발자는 기술된 요구사항을 참조하여 정보보호시스템을 개발할 수 있다.

1) 제 1 부 소개 및 일반모델

일반모델은 정보보호시스템의 평가원칙과 일반개념을 정의하고, 평가의 일반모델을 표현하는 공통평가기준의 소개부분 이다. 정보보호시스템의 보안목적을 표현하고, 정보보호시스템의 보안요구사항을 선택하여 정의하며, 정보보호시스템의 상위수준 명세를 작성하기 위한 구조를 소개한다. 또한 각 이용자 집단에 대하여 공통평가기준의 각 부의 유용성을 서술한다.[10]

2) 제 2 부 보안 기능 요구사항

제 2 부 보안기능 요구사항은 TOE 의 기능요구사항을 표준화된 방법으로 표현한 것으로 기능 컴포넌트들의 집합으로 이루어져 있다. 보안기능 요구사항은 11 개의 클래스로 이루어져 있으며 클래스별 내용은 다음과 같다. [11]

3) 제 3 부 보증 요구사항

제3부 보증요구사항은 TOE의 보증요구사항을 표준화된 방법으로 표현한 것으로 보증컴포넌트들의 집합으로 이루어져 있다. 3부는 보호프로파일과 보안목표명세서에 대한 평가기준을 정의하며, TOE의 보증수준에 대하여 공통평가기준에서 미리 정의된 척도를 소개하는데 이를 평가보증등급이라 한다.[12]

클래스명	클래스 제목	설 명
FAU	보안감사(Security Audit)	보안활동과 관련된 정보를 감지, 기록, 저장, 분리
FCO	통신(Communication)	데이터를 교환하는 주체의 신원을 감지
FCS	암호지원(Cryptographic Support)	암호 운용 및 키관리
FDP	사용자 데이터 보호 (User Data Protection)	사용자 데이터의 보호
FIA	식별 및 인증 (Identification & Authentication)	사용자의 신원확인 및 인증
FMT	보안관리(Security Management)	TSF 데이터, 보안속성, 보안기능의 관리
FPR	프라이버시(Privacy)	허가되지 않은 사용자에 의한 개인의 신원 및 정보의 도용방지
FPT	TOE 보안기능의 보호 (Protection of Trusted Security Functions)	TSF 데이터의 보호 및 관리
FRU	자원활용(Resource Utilization)	TOE의 가용자원을 확보
FTA	TOE 접근(TOE Access)	TOE에 대한 사용자 세션의 보호
FTP	안전한 경로/채널 (Trusted Path/Channel)	사용자와 TSF간 혹은 TSF 간의 안전한 통신채널 확보

<표6. 공통평가기준의 보안기능요구사항>

클래스명	클래스 제목	설 명
ACM	형상관리 (Configuration Management)	TOE의 무결성이 유지되고 있는지를 확인
ADO	배포와 운영 (Delivery and peration)	TOE의 안전한 배포, 설치, 운영에 필요한 수단, 절차 및 표준을 확인
ADV	개발(Development)	TOE 개발 과정의 일치성 및 완벽함을 확인
AGD	설명서(Guidance Documents)	TOE의 안전한 운영을 위한 지침서를 확인
ALC	생명주기 지원 (Life Cycle Support)	TOE의 생명주기와 관련된 사항을 확인
ATE	시험(Tests)	TOE가 기술요구사항을 만족하는 지를 확인
AVA	취약성 분석 (Vulnerability Analysis)	TOE의 개발 과정 중에 발견되지 않은 취약성,사용자에 의한 오용 등 잠재적인 취약성을 확인
APE	보호프로파일 평가 (Protection Profile Evaluation)	PP가 완전하고 모순이 없으며, 기술적으로 충분함을 보임
ASE	보안목표명세서 평가 (Security Target Evaluation)	ST가 완전하고 모순이 없으며, 기술적으로 충분함을 보임
AMA	보증의 유지 (Maintenance of assurance)	TOE나 보안환경이 변화에도 ST를 지속적으로 만족시킴을 보임

<표7.공통평가기준의 보증요구사항>

3. 새로운 평가 시험항목 제시

3.1 보안성 평가 모델
ISO/IEC 9126 의 보안성 평가 시험항목에 ISO/IEC 15408 의 보안 기능요구 사항중, 보안감사(Security Audit),사용자 데이터 보호(User Data Protection), 식별 및 인증 (Identification & Authentication)를 추가한 새로운 평가 시험항목을 추가한다.

3.2 보안감사 (Security Audit)

보안감사는 보안관련 행동에 관련된 정보의 인식,기록,저장,분석을 포함한다. 감사 레코드 결과는 어떤 보안관련 행동이 발생했는지에 대한 내용을 확인 할 수 있다.

보안 감사는 보안감사 데이터 생성,보안감사 사건저장 등의 2 가지 평가 기준을 가질 수 있다.

3.2.1 보안감사 데이터 생성 (Security Audit data generation)

보안감사 데이터 생성은 보안기능의 통제하에서 발생하는 보안관련 사건의 발생을 기록하는 요구사항을 정의한다. 보안감사 수준을 정의하고 보안기능에 의해서 감사 기록될 사건들을 명세하며, 여러 형태의 감사 레코드 내에서 제공되어야 하는 최소한의 감사 정보가 구현이 되어 있는지 평가한다.
측정방법은 <표 9>와 같은 항목으로 평가 한다.

측정항목	평가대상	측정유형
감사 데이터 생성 여부 (A)	P	Y/N/NA

<표9 보안성-보안감사 데이터생성>
세부평가 방법으로는 다음과 같다.

A: 감사 데이터 생성 여부 수
(1) 프로그램의 시동(Start-up) 과 종료 (shut-down)
(2) 보안기능 설정의 생성 및 수정에 대한 감사데이터 생성
(3) 비정상적인 종료에 대한 감사기록 생성
(4) 사건의 일시,유형,주체의 신원,사건의 결과(성공 또는 실패)

3.2.2 보안감사 사건 저장 (Security Audit event storge)

보안감사 사건저장은 안전한 감사 증적을 생성하고 유지할 수 있도록 하는 요구사항을 정의한다.

가. 감사 증적 보호(Protected audit trail storage)

감사 증적보호는 감사 증적에 중점을 두고 있다. 감사 증적은 인가되지 않는 삭제 및 또는 변경으로부터 보호 되어야 한다.

나. 감사 데이터의 가용성 보장 (Guarantees of audit data availability)

감사 데이터의 가용성 보장은 예상하지 않은 조건이 발생하여도 보안기능이 감사 데이터를 유지 하도록 하는 것을 명세한다.

다. 감사 데이터의 손실 방지 (Prevention of audit data loss)

감사데이터의 손실방지는 감사 증적 저장소가 포화되는 경우의 대응 행동을 명세한다.

위와 같은 평가 항목으로 평가한다. 측정 방법은 <표10> 과 같은 항목으로 평가한다

측정항목	평가대상	측정유형
보안 감사데이터의 저장 여부 (A)	P	Y/N/NA

<표10. 보안성-감사데이터 저장여부>

세부평가 방법으로는 다음과 같다.
A: 보안 감사데이터의 저장여부
(1) 감사저장 실패가 예상되는 경우에 취해야 할 대응행동의 유지 (추가,변경,삭제)
(2) 감사저장 실패의 경우에 취해야 할 대응행동의 유지 (추가,변경,삭제)
(3) 저장공간의 임계치를 초과 하였을 경우 대응행동
(4) 감사기록의 저장이 실패했을 경우의 대응 행동

3.3 사용자 데이터 보호(User Data Protection)

사용자 데이터 보호는 사용자 데이터의 보호와 관련된 제품의 보안 기능과 제품의 보안 기능 정책에 대한 요구사항을 명세를 포함한다. 사용자 데이터 보호는 사용자 데이터와 직접적으로 관련된 보안속성 뿐만 아니라 유입,유출,저장 하는 동안 제품내의 사용자 데이터를 중요 기능으로 구분된다.

사용자 데이터 보호는 접근통제 정책, 접근통제 기능,보안기능 통제 외부로의 사용자 데이터 유출,저장된 데이터의 무결성, 의 4 가지 평가 기준을 가질 수 있다.

3.3.1 접근통제 정책(Access Control policy)

접근통제 정책은 접근통제 보안기능정책을 식별하고 제품의 보안정책에 식별된 접근통제 부분을 구성하는 정책들의 통제 범위를 정의한다. 통제 범위는 정책의 통제하에 있는 " 주체" 와 정책의 통제하에 있는 " 객체" ,정책에 의해서 다루어 지는 통제된 주체와 통제된 객체 사이의 " 오퍼레이션" 등 세가지에 의해 특정 지어 진다. 측정방법은 <표 11>와 같은 항목으로 평가 한다.

측정항목	평가대상	측정유형
부분/완전한 접근통제 정책생성 여부(A)	D,P	Number
각 항목별 테스트 케이스의 성공의합(B)	P	Number

<표11. 보안성-접근통제 정책>

세부평가 방법으로는 다음과 같다.
A: 부분적인 접근 통제 정책 생성 여부
(1) 제품의 보안 기능을 부분적으로 통제 여부
(2) 제품의 보안 기능이 주체와 객체간의 모든 오퍼레이션에 대한 통제여부
B: 각 항목별 테스트케이스의 성공의 합
(1) 접근통제 규칙 생성에 대한 테스트케이스의 성공시 체크

3.3.2 접근통제 기능(Access Control function)

보안속성에 기반한 접근통제(Security attribute base access control)는 제품의 보안기능이 보안속성 및 속성그룹에 기반하여 접근통제를 수행 하도록 한다.

측정방법은 <표 12>와 같은 항목으로 평가 한다.

측정항목	평가대상	측정유형
접근통제 기능동작 여부(A)	P	Y/N/NA

<표12. 보안성-접근통제 기능>

세부평가 방법으로는 다음과 같다.
A: 접근통제 기능 동작 여부
(1) 보안기능 정책에 의해서 설정되어지는 보안기능 정상동작 여부
(2) 통제된 오퍼레이션을 이용하여 통제된 주체 와 통제된 객체간의 접근제어 되는지 여부
(3) 추가된 규칙에 의해서 통제된 주체와 객체간의 접근제어 기능 동작 여부

3.3.3 보안기능 통제 외부로의 사용자 데이터 유출

외부로 사용자 데이터 유출(Export to outside control)은 유출된 사용자 데이터에 대해서 데이터의 보안 속성이 유지되거나 무시될 수 있도록 제약한다.

측정방법은 <표13>와 같은 항목으로 평가 한다.

측정항목	평가대상	측정유형
사용자데이터유출(A)	P	Y/N/NA

<표13. 보안성- 사용자 데이터 유출>

세부평가 방법으로는 다음과 같다.
A: 보안속성 없이 사용자 데이터 유출
(1)보안기능정책에서 통제되는 사용자데이터를 외부로 유출할 경우 접근통제 기능 동작여부

3.3.4 저장된 데이터의 무결성

저장된 데이터의 무결성(Stored data integrity)은 보안기능의 통제 범위 내의 저장되어 있는 동안의 사용자 데이터 보호를 위해 사용된다. 무결성 오류는 메모리나 저장장치에 저장된 사용자 데이터에 영향을 미칠 수 있다.

측정방법은 <표14>와 같은 항목으로 평가 한다.

측정항목	평가대상	측정유형
저장된데이터의 무결성검사의 기능의수 (A)	D,P	Number
각항목별 테스트케이스의 성공의 합(B)	P	Number

<표13. 보안성- 데이터 무결성>

세부평가 방법으로는 다음과 같다.
A: 저장된 데이터의 무결성 검사를 위한 기능의 수
(1) 보안 기능은 모든객체에 대한 무결성에 대하여 저장된 사용자 데이터 검사 여부
(2) 보안 기능은 모든 객체에 대한 무결성에 대하여 저장된 사용자 데이터 검사 여부
(3) 무결성 오류 탐지시 대응행동 수행 여부
B: 각 항목별 테스트케이스의 성공의 합
(1) 무결성검사기능에 대한 테스트케이스의 성공시 체크

3.4 식별 및 인증 (Identification & Authentication)

식별 및 인증은 요청된 사용자의 신원을 설정하고 증명하기 위한 기능요구 사항 이며, 사용자가 적절한 보안 속성과 연관되는

이전에 사용자를 식별하는지 여부할것을 보장하도록 요구한다. 식별 및 인증은 사용자 신원의 결정 및 검증, 보안 제품과 상호 작용하기 위한 권한 결정, 및 사용자의 보안속성 에 사용된다. 식별 및 인증은 인증실패, 사용자인증, 사용자식별 의 3가지 평가 기준을 가질 수 있다.

3.4.1 인증실패 (Authentication)

인증실패는 실패한 인증시도의 회수 와 인증시도 실패시 보안 제품의 행동을 정의하기 위한 요구 사항을 포함한다.

측정방법은 <표14>와 같은 항목으로 평가 한다.

측정항목	평가대상	측정유형
실패한인증시도의한계치처리및행동의 모든 기능의 수(A)	P	Number
각 항목별 테스트케이스 성공율의합 (B)	P	Number

<표14. 보안성-인증실패 처리>

세부평가 방법으로는 다음과 같다.

A: 실패한인증시도의 한계치처리 및 대응행동의 모든기능의 수

(1) 관리자가 설정한 사용자 인증 실패 회수가 정상 동작 여부

(2) 사용자 인증 시도 실패 회수가 명시된 값을 초과 하였을 경우 행동 동작여부

(3) 정상 상태로의 회복 여부

B: 각 항목별 테스트케이스 성공율의 합

(1)인증실패 및 한계치에 대한 테스트케이스를 시험한성공한경우를 체크

3.4.2 사용자인증(User authentication)

사용자 인증은 보안기능이 지원하는 사용자 인증 메커니즘 유형을 정의 하며, 인증메커니즘이 기반해야 하는 요구 속성들을 정의한다.

측정방법은 <표15>와 같은 항목으로 평가 한다.

측정항목	평가대상	측정유형
인증 (A)	P	Y/N/NA
모든 행동 이전에 사용자 인증(B)	P	Y/N/NA
위조할 수 없는 인증 (C)	P	Y/N/NA
재사용 방지 인증 메커니즘(D)	P	Y/N/NA

<표15. 보안성-사용자 인증>

세부평가 방법으로는 다음과 같다.

A : 인증

(1) 관리자에 의한 인증 데이터 관리 여부

(2) 관련 사용자에 의한 인증 데이터 관리 여부

B : 모든 행동이전에 사용자 인증

(1) 사용자가 인증되기 전에 수행할수 있는 행동목록 관리 여부

C : 위조할 수 없는 인증

(1) 모든 사용자로부터 부정한 인증 데이터의 탐지 여부

(2) 모든 사용자로부터 부정한 데이터에 대한 검사 결과와 취해진 모든 즉각적인 대책 여부

D: 재사용 방지 인증 메커니즘

(1) 인증 데이터의 재사용 시도 방지 여부

3.4.3 사용자 식별 (User identification)

사용자 식별은 제품의 보안 기능에 의해 관리되어야 하고 사용자 인증을 요구하는 다름 노든 행동을 수행하기 전에 사용자를 식별 하도록 요구 되는 조건을 정의 한다.

측정방법은 <표16>와 같은 항목으로 평가 한다.

측정항목	평가대상	측정유형
식별을 위한 모든기능의 수(A)	P	Number
항목별 테스트케이스의 성공율의 합(B)	P	Number

<표16. 보안성 - 사용자 식별>

세부평가 방법으로는 다음과 같다.

A : 식별을위한 모든 기능의 수

(1) 사용자가 식별하기 전에 사용자를 대신하여 수행될 행동목록 허용 여부

(2) 수행될 행동목록 전에 각 사용자를 성공적으로 식별하는지 여부

(3) 보안 제품은 사용자를 대신하여 모든 행동을 허용 여부

B : 항목별 테스트케이스 성공율의 합

(1) 사용자 식별을에 대한 테스트 케이스를 시험하여 성공한 경우 체크

위와 같이 새로운 3가지 주항목에 9가지 부항목 16가지 세부 매트릭스와 29개의 체크리스트를 추가하였다.

기존 ISO/IEC 9126 품질특성중 기능성의 부특성인 보안성에 세부 매트릭스의 수와 새로이 추가된 시험항목의 매트릭스의 수를 정리하면 <표17>과 같다.

평가항목 \ 평가모델	ISO/IEC9126	새로운 추가된 평가모델	합계
부특성항목 수	4	9	13
세부메트릭 수	15	29	44

<표17. 새로운평가모델과 기존 모델의 항목 수>

<표17>과 같이 기존의 15개의 매트릭스를 가지고 소프트웨어형 보안 제품을 평가 하였으나, 새로운 평가 모델의 매트릭스를 적용하면 총 44가지의 매트릭스를 확대 되어지며, 평가의 부특성 영역도 증가되었다.

4. 새로운 평가 모델에 대한 검증

논문에서 추가된 보안성 평가 시험항목은 소프트웨어 형 보안 제품의 최소한의 기능 요구 사항을 기반으로 작성된것이다.

기존 ISO/IEC 9126 기반의 시험 항목 메트리스와 추가된 16가지 세부 매트릭스를 가지고 실제 제품에 적용하여 매트릭스에서 도출된 결과 값을 비교하겠다. 적용 사례는 제시하면 다음과 같다.

A사의 소프트웨어는 보안용 S/W 중 DB 보안과 관련된 소프트웨어 이다.

시험 대상은 외부침입에 대한 DB의 안전뿐만 아니라 인가된 사용자의 실수나 악의적인 접근으로부터 데이터를 보호하고, 모든 DB Quary 데이터를 내부 로그서버에 저장하며, 관리툴로 로그조회 기능을 통해 실시간 모니터링 및 감사 데이터의 조회,통계 를 할 수 있는 제품이다.

ISO/IEC 9126 품질특성중 기능성의 부특성이 보안성 기준으로 총 15개의 세부매트릭스 항목으로 평가가 가능했다.

평가대상 \ 측정항목		항목수	평가결과항목수
보안성	접근통제점검표(A)	8	8
	접근감사점검표(B)	7	7
측정치 (B/A)		0.87	

<표18. 보안성-접근통제/감사 매트릭스 평가표>

<표18>은 기존에 사용 되었던 보안성의 접근통제 매트릭스 중 일부분 이다. 측정치는 소프트웨어 품질 평가에서 사용하는 측정치 매핑방법을 이용했다.[3]

측정치는 품질기준을 만족하는 점검표의 기능의(Y) 수를 측정한 뒤 항목수로 나눈 결과 값이다.

여기서 B 는 아래와 같은 계산식으로 계산 된다. 또한 측정 결과는 Positive 매트릭스다. 이는 측정치가 1에 가까울수록 좋은 품질을 의미하는 값으로, 다음과 같은 범위를 갖는다.

$$0 \le \text{측정치} \le 1$$

측정 결과 테스트 대상 소프트웨어의 접근통제 측정값이 0.87로 높게 나왔다. 하지만 보안 기능중 접근통제에 대한 측정 기준

이기 때문에 모든 보안성을 만족 한다고 할 수는 없다.
아래의 <표19>는 새로운 평가 모델을 적용한 결과 값이다. 측정 방법은 소프트웨어 품질 평가에서 사용하는 측정 매핑방법과 동일하게 적용하였다.

평가대상 \ 측정항목		항목 수	평가결과 항목 수
보안감사	감사데이터생성	4	4
	보안감사 사건 저장	4	4
사용자데이터 보호	접근통제정책	2	1
	측정치	0.5	
	접근통제기능	3	3
	보안기능통제 외부로의 사용자데이터 유출	1	1
	저장된 데이터의 무결성	3	2
	측정치	0.66	
식별 및 인증	인증 실패	3	3
	측정치	1	
	사용자 인증	6	4
	측정치	0.66	
	사용자 식별	3	2
	측정치	0.66	

<표 19. 새로운 평가 모델 적용한 결과값>

새로운 기준으로 측정 결과 보안감사에서는 모든 조건을 만족하였고,사용자 데이터 보호 체크조건 중 접근통제를 제외한 나머지 항목은 0.5 등 그리 좋지 않은 결과 값을 보여 주고 있다. 또한 식별 및 인증에서는 인증실패를 제외한 나머지 항목이 0.66 으로 좋지 못한 값을 보여 주고 있다.

5. 결론

소프트웨어의 범위가 광범위해 지면서, 소프트웨어 형 방화벽 등 기존의 하드웨어 일체형 장비 위주에서 소프트웨어 형으로 변하고 있는 추세이며, 이러한 추세에 맞춰 소프트웨어 형 보안 제품의 품질에 대한 관심도 같이 증가하고 있다.
몇 가지 보안 제품에 대하여 한국정보보호 진흥원에서 국제 공통 평가 기준 (CC)를 적용하여 보안 제품을 평가 및 인증을 하고 있지만, 평가 및 인증의 대상 제품 군이 한정 되어 있으며, 제품의 평가 및 요구사항이 많아 제품을 평가 및 인증을 받기까지 많은 시간이 소요된다. 앞으로 평가 및 인증 대상 제품군을 추가 한다고 하였지만, 모든 보안 제품에 국제 공통 평가 기준을 적용하여 평가 인증을 하기에는 많은 시간이 소요 될 것이다.
본 논문은 ISO/IEC 9126 의 평가모델로 제품의 평가를 하고 있는 평가 매트릭스 내용중 기능성의 부특성인 보안성의 평가 항목을 넓히기 위해 개발에 관한 것이다.
본 논문에서 제안하고 있는 평가 모델은 ISO/IEC 15408 (CC)에서 요구 하는 요구 사항 중 소프트웨어 형 보안 제품에 맞게. 평가 항목을 도출해 내는 과정에서 제품의 평가 매트릭스 내용을 수정하여, 제품의 세부 평가 내용을 도출 할 수 있었다.
이러한 평가 모델의 보완으로 소프트웨어 형 보안 제품의 품질이 향상이 될 수 있을 것이다.
하지만, ISO/IEC 9126의 평가 모델 및 평가 방법 은 국제 표준 기구에서 평가 모델 및 평가 방법이 보완 되어야 한다. 이러한 평가 모델의 보완을 위하여 각 항목별 세부 매트릭스에 대한 연구가 더 많이 진행이 되어야 할 것이다.
그러한 과정을 통해 보다 완전한 소프트웨어형 보안 제품의 평가 모델이 마련 될 수 있을 것이다.
이러한 연구들은 궁극적으로 소프트웨어형 보안제품의 품질을 높일 수 있는 기반이 될 것이다.

참고 문헌

[1]ISO 9126-1, Software engineering-Product quality-Part 1: Quality model, 2000
[2]한국전자통신 연구원 품질보증연구팀, S/W 품질검사표, 한국전자통신연구원. 2000
[3]한국전자통신연구원 품질보증연구팀, S/W 시험을 위한 Evaluation Module , 한국전자통신연구원. 2000
[4]ISO/IEC 9126 Software product evaluation- Quality Characteristics and guidelines for their use, 1994
[5] 국내 · 외 정보보호시스템 평가 동향, 한국정보보호센터, 1999.12
[6] 국제 공통 평가 기준 V2.0(번역서), 한국정보보호센터, 1998.7
[7]정보통신부 고시 제 2000-14호, 정보통신망 침입차단시스템평가기준,2000.2.17
[8] 정보통신부 고시 제 2000-62호, 정보통신망 침입탐지시스템평가기준,2000.7.29
[9]정보통신부 고시 제2001-24호, 정보보호시스템 평가 · 인증 지침, 2001.4.24
[10]ISO/IEC 15408-1, Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model, 1999.12.1
[11]ISO/IEC 15408-2, Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements, 1999.12.1
[12]ISO/IEC 15408-3, Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance requirements, 1999.12.1
[13]국내 · 외 정보보호시스템 평가 동향, 한국정보보호센터, 1999.12
[14]ISO/IEC 25010(new) Software engineering: Software product Quality Requirements and Evaluation(SQuaRE) - Quality model 2005.