논문 2010-1-3

정보보호제품 품질 평가를 위한 리스크 기반의 메트릭 설계

윤여웅*, 이상호**

A Design of Risk-Based Metrics for Evaluating the Quality of Information Security Products

Yeo-Wung Yun*, Sang-Ho Lee**

요 약

정보보호제품 사용자는 보안성과 성능을 포함하여 좋은 품질의 정보보호제품을 요구하고 있으나 다양한 정보보호제품의 품질을 평가하기 위한 품질 모델과 메트릭에 대한 연구와 정보보호제품의 품질에 대한 평가 사례도 찾아보기 어렵다.

본 논문에서는 정보보호제품 품질의 리스크를 분석한 후 품질 모델을 새롭게 정의하였고 정의된 품질모델은 7가지 특성과 24가지 부특성을 가진다. 또한, 정보보호제품의 품질평가에 사용가능한 62가지 공통 메트릭과 45가지 선택 메트릭을 설계하였다.

Abstract

While users of information security products require high-quality products that are secure and have high performance, there are neither examples for evaluating the quality of information security products nor studies on the quality models and metric for the quality evaluation.

After analyzing the risks of information security products' quality, a new quality model that possesses 7 characteristics and 24 sub-characteristics has been defined. In addition, metrics designing of 62 common and 45 optional metrics that can be used to evaluate the quality of information security products are introduced.

Keywords : 정보보호제품, 품질 모델, 품질평가, 품질 메트릭

Ⅰ. 서론

정보사회의 급속한 발달은 인가되지 않은 불법 사용자로 인한 정보시스템 파괴, 개인의 프라이버시 침해, 지적재산권 침해, 불건전 정보의 유통 등의 역기능을 발생시키고 있으며, 중요 정보

* (주)한국아이티평가원
(email: ywyun@ksel.co.kr)
** 충북대학교
접수일자: 2010.2.16 수정완료: 2010.5.2

를 소유한 인터넷 사용자는 이러한 역기능에 대응하기 위하여 정보보호제품 도입 등을 통한 보안대책을 마련하고 있다[1].

초기 정보보호제품에 대한 사용자 요구는 보안성에 집중되었다. 사용자는 패킷필터링 및 프록시 기반의 접근통제를 정확히 수행할 수 있는 침입차단시스템과 전송되는 네트워크 패킷을 모두 수집하여 침입 행위를 정확히 탐지할 수 있는 침입탐지시스템 등의 정보보호제품을 요구하였다. 그러나, 인터넷 환경이 대용량 네트워크 환경으로 전환되면서 사용자 요구는 정보보호제품이 보안성을 정확히 수행하는 것만으로 충족되지 못하였다. 침입차단시스템의 경우 보안성을 보장한다고 하더라도 대용량 네트워크 환경에서 전송되는 많은 패킷을 처리하지 못하면 무용지물이 되기 때문이다. 따라서, 사용자는 정보보호제품의 보안성뿐만 아니라 대용량 네트워크 환경에서도 지속적으로 보안성을 수행할 수 있는 높은 성능 등을 제공할 수 있는 좋은 품질의 정보보호제품을 요구하고 있다.

정보보호분야와는 달리 소프트웨어에서는 오래전부터 품질 평가와 관련 연구들이 진행되었으며, 소프트웨어 발전 추세에 따라 일반 소프트웨어뿐만 아니라 패키지용 소프트웨어, 임베디드용 소프트웨어, 의료용 소프트웨어 등을 평가하기 위한 품질 모델과 메트릭에 대한 연구들이 있다[2,3,4,5,6,7,8,9,10,11,12]. 그러나, 기존 연구는 소프트웨어군별로 고정된 메트릭을 생성하고 있기 때문에 다른 유형의 소프트웨어에 적용하기 위한 추가적인 연구가 필요하다.

소프트웨어에 대한 완벽한 시험은 불가능하며, 정보보호제품 품질에 대한 시험도 동일하다. 특히, 소프트웨어 내의 내부조건이 무수히 많을 수 있고 하나의 입력이 가질 수 있는 모든 값의 조합이 무수히 많기 때문에 모든 가능한 조합을 시험하는 불가능하다. 따라서 완벽한 시험을 대신하여 리스크(Risk) 분석과 리스크 분석을 통해 결정된 우선순위에 따라 시험을 하는 리스크 기반 시험 전략이 필요하다. 품질 평가 메트릭에 대한 기존 연구에서는 리스크 분석을 통하여 산정된 리스크별로 얼마나 많은 메트릭을 생성할 것인지가 고려되지 않았다. 따라서, 사용자 요구에 따라 다양한 정보보호제품 품질 평가를 위하여 기존 연구의 품질 모델과 메트릭은 적합하지 않으며, 메트릭 생성 시 품질 특성별 리스크가 고려되지 않아 기존 연구결과를 정보보호제품 품질 평가에 적용할 수 없기 때문에 품질 특성별 리스크에 대한 분석이 추가적으로 필요하다.

또한, 정보보호제품 보안성 및 성능은 시험 및 평가기관에서 특정 품질의 특성별로 시험 및 평가가 이루어지고 있으나[5,7,18,21], 보안성 및 성능 등을 포함한 정보보호제품 품질을 포괄적으로 검증할 수 있는 기준 및 제도가 마련되어 있지 않고 정보보호제품 품질 평가를 위한 품질 모델과 메트릭에 대한 연구가 선행되지 않아 정보보호제품에 대한 품질 평가는 이루어지고 있지 않다. 따라서, 사용자들이 정보보호제품의 보안성과 성능을 정확하게 비교하고 선택할 수 있도록 정보보호제품의 품질을 평가하기 위한 체계적인 방안에 대한 연구가 필요하다.

따라서, 이 논문에서는 2장에서는 품질 평가와 관련된 연구를, 3장에서는 품질 모델을, 4장에서는 다양한 정보보호제품의 품질을 평가하기 위한 정보보호제품 품질별 리스크가 반영된 품질 평가 메트릭을 제안하고자 한다.

II. 관련 연구

2.1 소프트웨어 품질 관련 표준

소프트웨어 품질에 대한 표준은 ISO/IEC

JTC1이 국제 표준화를 주도하고 있으며, 제품 평가 분야, 프로세스 평가 분야, 품질시스템 구축 분야로 이루어지고 있다.

ISO/IEC 9126은 소프트웨어 품질 특성과 척도에 관한 지침으로 사용자 관점에서 소프트웨어에 관한 품질 특성(Quality Characteristics)과 품질 부특성(Sub-Characteristics)을 정의하고 있다[13]. ISO/IEC 14598은 소프트웨어 제품의 품질을 측정하거나 평가하는데 6부분으로 나누어 정의하고 있으며[14], ISO/IEC 25000(SQuaRE)은 소프트웨어 제품 품질 요구사항 및 평가라고 부르는 국제표준으로서 SQuaRE 모델 내에 크게 6개 부분으로 구성되어 있다[15,16].

2.2 소프트웨어 품질 평가

미국, 유럽 등 주요 선진국에서는 이미 오래전부터 소프트웨어 품질의 중요성을 인식하여 품질 문제를 해결할 수 있는 시험·인증이 시행되었다[5,7].

미국은 민간주도의 소프트웨어에 대한 다양한 인증 부여를 수행하고 있는데, 대표적인 인증기관으로 VeriTest, NSTL, NTS/XXCAL, AppLabs 등이 있으며, 덴마크의 DELTA는 1982년부터 ISO/IEC 9126 품질특성을 기반으로 하여 중요한 프로세스 통제 및 실시간 소프트웨어의 기능성을 평가하였다. 독일의 TuViT은 ISO/IEC 9126, ISO/IEC 14598에 기반을 둔 IT제품 평가 및 인증 서비스, IT 프로젝트 품질관리 및 컨설팅 업무를 수행한다. 프랑스의 Aquitaine-valley사가 프랑스 표준원인 AFNOR로부터 NF Logiciel 마크 인증 프로세스를 위임받아 소프트웨어 제품 평가 및 인증 업무를 수행한다. 프랑스의 인증기관인 COFRA는 Aquitaine-valley사가 이러한 인증기관으로 역할을 수행할 수 있도록 인정한다. 영국은 정부 주도의 표준화 기관인 영국표준원(BSI)에서 특정한 제품이 품질요구사항을 만족하는지를 확인하고, 일본의 JQA는 1957년 경제통상산업부 산하에 설립된 시험평가기관으로 보안 소프트웨어 및 시스템에 대한 인증을 수행한다.

국내의 경우는 한국정보통신기술협회에서 2001년부터 패키지 소프트웨어, 모바일 소프트웨어, 컴포넌트 소프트웨어, 웹기반 소프트웨어, 임베디드 소프트웨어 등 품질 평가를 수행하고 있으며, 한국산업기술시험원은 2003년부터 산업용 소프트웨어 표준적합성 인증을 실시하였으나 굿 소프트웨어 인증으로 통합하여 운영하고 있다.

2.3 정보보호제품 보안성 평가

정보보호제품에 대한 보안성 평가는 ISO/IEC 15408에 정의된 공통평가기준을 기반으로 정보보호제품의 보안성과 이에 적용된 보증수단이 이러한 요구사항들을 만족하는지에 대한 신뢰도를 확인하는 것으로 전 세계적으로 널리 시행되고 있다[17,18]. 정보보호제품 평가기관에서는 공통평가기준을 기반으로 다양한 정보보호제품의 보안성을 평가하고 있다.

2.4 정보보호제품 성능 평가

성능평가는 정보보호제품의 견고성, 효율성 등을 확인하는 것으로 시험의뢰자의 요구에 따라 정보보호제품의 전체적인 제품 성능뿐만 아니라 제품을 구성하는 일부 계층 및 기능의 성능을 평가할 수도 있다.

톨리(Tolly) 그룹은 1989년에 설립된 미국의 사설 시험전문기관으로 품질보증 시험, 알파 또는 베타 시험, 비교 벤치마크, 톨리 업투 스펙인증, 톨리 검증인증, 톨리 시험인증 등의 시험 및 인증을 수행하고 있다.

NSS 그룹은 1991년 영국에서 설립된 보안제품 전문 평가기관으로 주로 IDS, IPS, Firewall 등의 네트워크 보안장비들의 시험을 수행하고 기능 및 성능에 대한 평가를 실시하고 있다.

ICSA는 1991년에 설립된 미국의 사설 시험기관으로써 암호장비, 침입차단시스템, 침입탐지시스템, IPSec, 안티바이러스, PKI 등 다양한 정보보호제품에 대한 인증을 실시하고 있다.

한국정보통신기술협회는 정보통신 관련 장비의 공정한 시험 및 인증 서비스를 제공하고 있으며, 네트워크 장비 기능 확인 시험, 네트워크 장비 성능 평가시험, 네트워크 장비 개발지원 시험, 네트워크 장비 상호운용성 시험 등을 수행하고 있다.

또한, 미국의 Sandia, 산호세 주립대학 NBTC, 영국의 NPL, 독일의 GISA 등에서는 바이오제품에 대한 성능 시험을 수행하고 있다[21].

2.5 기존 품질 모델 및 메트릭 문제점

소프트웨어 품질을 평가를 위한 메트릭은 산업용 소프트웨어, 임베디드 소프트웨어, 의료용 소프트웨어, Open Source 소프트웨어, 보안 소프트웨어, 인트라넷 소프트웨어 등 다양한 소프트웨어 품질에 대한 모델 및 메트릭에 대한 연구가 진행되었다[2,3,4,5,6,7,8,9,10,11,12]. 지금까지의 기존 소프트웨어 품질 평가를 위한 품질 모델 및 메트릭에 대한 연구는 특정 소프트웨어군에 종속된 고정된 메트릭을 생성하여 다양한 소프트웨어에 적용되지 못하고, 새로운 유형의 소프트웨어에 대한 품질 평가를 위해서는 추가적인 연구가 필요했기 때문에 정보보호제품 품질 평가를 위해서도 기존 연구를 그대로 적용할 수 없으며 추가적인 연구가 필요하다.

또한, 품질 평가자가 생성된 품질 평가 메트릭을 통하여 품질 평가를 수행할 때 무한정 평가기간이 부여되지 못하기 때문에 일정 기간 내에 보다 적합한 품질 평가를 하기 위해서는 리스크에 대한 고려가 필수이다. 완벽한 시험은 불가능하므로 리스크가 고려되지 않으면 필요한 메트릭이 누락되거나 불필요한 메트릭이 포함될 수 있다. 따라서, 정보보호제품의 품질 평가를 위한 품질 메트릭 생성 시 정보보호제품 품질 특성에 따른 리스크가 고려되어야 한다.

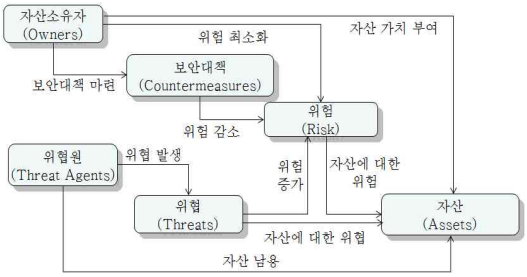
따라서, 기존 소프트웨어 품질 관련 연구 결과는 보안성과 성능 등이 중요한 다양한 정보보호제품의 품질을 평가하기 위한 품질 모델 및 메트릭으로 활용하는 것은 불가능하기 때문에 정보보호제품 품질 평가를 위한 품질 모델 및 메트릭에 대한 체계적인 연구가 필요하다.

III. 정보보호제품 품질 모델

3.1 정보보호제품 정의

정보보호는 정보의 수집, 가공, 저장, 검색, 송신, 수신 중 발생할 수 있는 정보의 훼손, 변조, 유출 등을 방지하기 위한 관리적·기술적 수단을 마련하는 것으로, 내·외부의 위협요인들로부터 네트워크, 시스템 등의 하드웨어, 데이터베이스, 통신 및 전산 시설 등 정보자산을 안전하게 보호하고 운영하기 위한 일련의 행위나 개인 정보 유출, 남용을 방지하기 위한 일련의 행위들이다.

중요 정보를 소유한 인터넷 사용자는 (그림 1)과 같이 위협원으로부터 발생되는 위협들로부터 운영 환경 내의 자산을 보호하기 위하여 자산의 가치를 부여하고 위험을 감소시키기 위해 다양한 보안대책을 마련하며, 보안대책은 다양한 정보보호제품의 활용을 통하여 구현되며[17], 정보보호제품의 정의는 (정의 1)과 같다.



(그림 1) 정보보호 개념도

(정의 1) 정보보호제품 : 정보의 수집, 가공, 저장, 검색, 송신, 수신 중 발생할 수 있는 정보의 훼손, 변조, 유출 등을 방지하기 위한 관리적·기술적 수단

3.2 정보보호제품 품질 요구사항

정보보호제품은 일반 소프트웨어와 달리 가장 중요한 품질이 보안성이며, 낮은 성능을 가진 정보보호제품은 대용량 네트워크 환경에서 운영되지 않을 수 있으므로 성능적인 요소를 포함한 아래와 같은 정보보호제품의 특성이 고려되어야 한다.

3.2.1 안전한 자산 보호 기능

정보보호제품은 운영 환경 내의 자산을 안전하게 보호하기 위하여 다양한 보안성을 제공하며, 정보보호제품이 제공하는 보안성은공통평가기준의 보안기능요구사항을 기반으로 11가지로 구분하였고, 세부적인 보안성을 55가지로 정의하였다[17]. 다양한 정보보호제품에서 제공되는 정의된 보안성은 품질 평가 시 보안성이 정확하게 제공되는지 확인되어야 한다.

3.2.2 높은 성능

정보보호제품은 효율성을 평가하기 위해서 매우 다양한 성능 요소가 적용가능하며, 일반 소프트웨어는 필요할 때 구동시켜서 사용하지만 정보보호제품은 운영 환경 내의 자산을 보호하기 위해 항상 구동되어야 하며, 일부 정보보호제품에 대한 성능 요소가 정의되어 있다. 침입차단시스템의 경우 채널을 통하여 실제로 전송 가능한 처리율(throughput)과 전송된 정보가 목적지까지 전달되는데 걸리는 시간인 지연(delay)으로 정의하고 있다[20]. 지문인식시스템의 경우도 타인수락율, 본인거부율, 이미지 등록 및 획득 시 실패한 비율, 특정점 추출 및 비교에 걸리는 시간 등을 제시하고 있다[21].

3.2.3 사용편의성

정보보호제품의 사용자는 한 조직의 정보보호 담당자처럼 정보보호 관련 많은 지식과 경험을 가진 사용자일 수도 있지만 일반 PC 사용자처럼 정보보호에 대한 지식과 경험이 거의 없는 사용자 등 누구나 정보보호제품의 사용자가 될 수 있다. 따라서, 정보보호제품을 사용하는 사용자라면 누구나 정보보호제품을 쉽고 편리하게 사용할 수 있도록 하기 위해 기능, 인터페이스, 메시지, 도움말 등에 대한 이해와 기능 습득이 용이해야 한다.

3.2.4 신뢰성

정보보호제품은 항상 동작되는 것을 보장하기 위하여 정보보호제품 사용 시 제품을 다운시키는 결함이나 심각한 고장을 발생시키는 결함에 대해 자체적인 대응 능력을 가져야 하며, 사용자의 오

조작으로 인해 발생할 수 있는 심각한 오류를 사전에 방지할 수 있도록 대응할 수 있어야 한다.

3.2.5 유지보수성

정보보호제품은 새로운 취약점이 항상 발생될 수 있으며, 새로운 취약점이 발생된 경우 정보보호제품을 업그레이드하여 정보보호제품이 새로운 취약점에 대응할 수 있도록 하여야 한다. 이러한 업그레이드를 통한 유지보수에 많은 시간이 소요된다면 운영 환경 내 자산의 보호를 보장할 수 없을 것이다.

3.2.6 통합 호환성

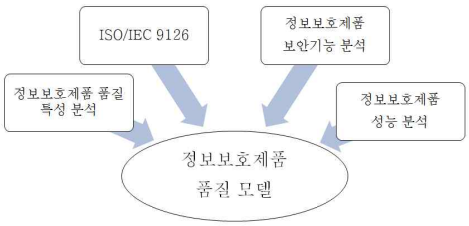
정보보호제품은 설치 및 제거 절차에 따라 정보보호제품을 성공적으로 설치 및 제거할 수 있어야 하며, 정보보호제품을 업그레이드하는 경우 이전 버전에서 사용하던 기능과 데이터를 그대로 사용할 수 있어야 한다. 또한, 다양한 보안성을 가진 정보보호제품이 통합되어 유기적으로 동작되는 것이 필요하다.

3.3 정보보호제품 공통 보안기능

정보보호제품의 품질 모델 정의를 위하여 정보보호제품이 제공하는 공통 보안기능에 대한 도출이 필요하며, 이 논문에서는 네트워크 정보보호제품군인 침입차단시스템과 침입탐지시스템, 정보보호 기반 제품군인 지문인식시스템, 컴퓨팅 정보보호제품군인 운영체제보안시스템의 보안성을 분석하여 정보보호제품이 공통적으로 제공해야 하는 보안성을 보안감사성, 신분확인성, 보안관리성, 자체보호성으로 정의한다[22,23,24,25].

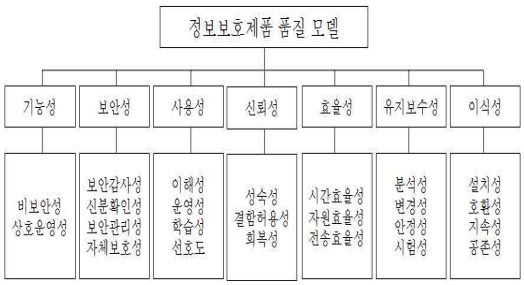
3.4 정보보호제품 품질 모델

정보보호제품의 품질 모델은 (그림 2)와 같이 정의된 정보보호제품 품질 특성을 토대로 정보보호제품의 보안성과 성능을 분석하여 ISO/IEC 9126에서 정의된 소프트웨어 품질 모델을 확장하여 정의한다.



(그림 2) 정보보호제품 품질 모델 개념

정의된 정보보호제품의 품질 모델은 일반 소프트웨어와 달리 보안성과 성능 관련 품질이 매우 중요하기 때문에 ISO/IEC 9126에서 정의된 소프트웨어 품질 모델을 기반으로 (그림 3)과 같이 7개의 주특성과 24개의 부특성으로 정의한다.



(그림 3) 정보보호제품 품질 모델

기능성은 정보보호제품이 제공하는 보안성 외에 하드웨어 정보 및 제품 상태 보기 등의 비보안성의 구현이 정확한지와 다른 제품과 상호작용을 하는 기능이 정상적으로 동작하는지를 평가한다.

보안성은 정보보호제품이 특정 정보보호제품이 제공해야 할 최소한의 보안성을 도출하여 부특성으로 정의한다. 보안성의 부특성은 다양한 정보보호제품에서 공통적으로 제공되어야 하는 최소한의 보안성으로서 보안감사성, 신분확인성, 보안관리성, 자체보호성을 포함한다.

사용성은 이해성, 운영성, 학습성, 선호도를 통하여 정보보호제품 사용 시 사용자가 발생한 오류를 쉽게 교정하고 현재 수행되고 있는 작업의 진행상태를 알 수 있어야 한다.

신뢰성은 성숙성, 결함허용성, 회복성을 통하여 오류 발생 시 빠른 시간 내에 복구되어 운영의 연속성을 제공해야 한다.

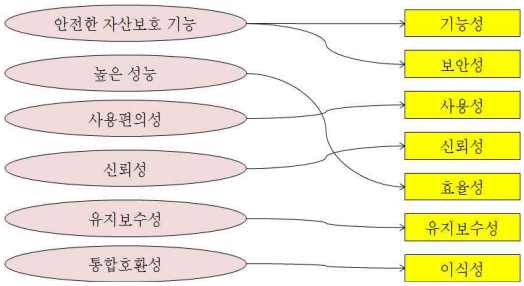
효율성은 정보보호제품에 특정 입력을 제공한 후 결과를 빠른 시간 내에 얻을 수 있어야 하며, 메모리, 디스크, CPU, 입출력장치 등 적은 자원의 사용으로 효율성을 극대화해야 한다.

유지보수성은 분석성, 변경성, 안정성, 시험성을 통하여 시뮬레이션 기능, 사전 검사 기능 등 정보보호제품이 제공하는 자체 기능에 대해 시험할 수 있어야 하며 규칙 업데이트 등 새로운 취약점에 대응할 수 있어야 한다.

이식성은 설치성, 호환성, 지속성을 통하여 설치 및 제거가 용이하고, 다양한 하드웨어나 소프트웨어뿐만 아니라 조직의 기반구조나 하드웨어 장치, 네트워크 장비, 운영체제 등의 환경에서 사용가능해야 하며, 동일한 환경에서 동일한 목적으로 사용하기 위하여 정보보호제품을 업그레이드하는 경우 이전 버전에서 사용하던 기능과 데이터를 그대로 사용할 수 있어야 한다.

정보보호제품 품질 특성과 정보보호제품 품질 모델간의 관계는 (그림 4)와 같다.

정보보호제품 품질 모델의 7개의 주특성은 정보보호제품 품질 요구사항을 모두 만족하도록 정의하며 이러한 주특성별 품질 평가를 위한 리스크 기반의 메트릭을 설계하고자 한다.



(그림 4) 정보보호제품 품질 특성과 품질 모델간 관계도

IV. 리스크 기반의 메트릭 설계

4.1 정보보호제품 품질 리스크 산정

소프트웨어 테스팅 분야에서는 완벽한 테스팅이 불가능하므로 리스크를 고려한 효율적인 테스팅을 권고하고 있으나, 기존 연구에서는 소프트웨어 품질 평가 메트릭을 생성할 때 리스크를 전혀 고려하지 않고 메트릭을 생성하였다.

그러나, 정보보호제품의 품질을 평가하는데 평가 인력, 평가 기간 등의 자원이 무한한 것이 아니므로 정보보호제품 품질이 검증되지 않았을 경우 품질 특성별로 정보보호제품 전체에 미칠 수 있는 리스크가 상이하므로 정보보호제품의 품질 평가 메트릭을 설계할 때 리스크에 대한 고려가 필수적이다.

소프트웨어 분야에서는 제품 리스크를 "소프트웨어나 시스템에서 의도치 않은 향후 이벤트나 위험 요소가 존재하는 잠재적인 장애 영역(Potential failure areas)"으로 정의하고 있으며 [19], 이 논문에서는 정보보호제품 품질 리스크를 (정의 2)와 같이 정의한다.

(정의 2) 정보보호제품 품질 리스크 : 정보보호제

품에서 의도치 않은 이벤트나 위험 요소가 발생하여 제품의 취약점을 발생시킬 수 있는 잠재적인 장애 영역

정보보호제품 품질 리스크는 (수식 1)과 같이 산정한다.

(수식 1) 정보보호제품 품질 리스크(RK : Risk) = 정보보호제품 품질의 장애 발생 가능성(LH : Likelihood) × 정보보호제품 품질의 영향(IP : Impact)

산정된 정보보호제품 품질 리스크를 통하여 장애발생 가능성과 영향이 커서 리스크가 큰 품질에 대해서는 품질 평가를 위한 메트릭을 다수 생성하여 적용하고, 장애발생 가능성과 영향이 작아 리스크가 작은 품질에 대해서는 품질 평가를 위하여 적은 수의 메트릭을 생성하여 적용한다. 정보보호제품 품질에 대한 리스크를 산정하기 위하여 정보보호제품 평가 전문가를 통한 리스크 산정 방식을 채택한다. 정보보호제품 평가 전문가는 한국인터넷진흥원 등 정보보호제품 선임평가자 10인을 선정하였으며, 선정된 전문가를 대상으로 정보보호제품 품질별 리스크에 대한 설문조사를 통하여 정보보호제품 품질 리스크를 산정하였다.

정보보호제품 품질 리스크 설문조사 집계는 [표 1]과 같으며, 장애발생가능성과 영향에 대한 설문조사 결과이다.

[표 1] 정보보호제품 품질 리스크 설문조사 집계

설문자	평가자1		평가자2		평가자3		평가자4		평가자5		평가자6		평가자7		평가자8		평가자9		평가자10	
소속	KISA		KISA		KISA		KISA		KISA		KISA		KISA		KISA		KISA		KSEL	
구분	LH	IP	LH	IP	LH	IP	LH	IP	LH	IP	LH	IP	LH	IP	LH	IP	LH	IP	LH	IP
기능성	1	2	1	1	2	2	1	2	1	1	2	2	1	1	2	1	1	1	1	1
보안성	1	3	3	3	3	3	3	3	3	2	3	3	3	3	3	3	1	3	3	3
사용성	2	3	1	3	1	3	3	2	2	2	1	3	2	2	2	2	2	3	1	3
신뢰성	2	2	1	2	2	1	2	3	2	2	3	2	1	2	1	3	2	3	2	2
효율성	1	2	2	2	1	3	3	3	1	3	2	3	1	1	2	2	3	3	3	3
유지 보수성	1	2	1	2	1	1	2	2	3	1	2	1	1	1	1	1	1	3	1	1
이식성	2	3	2	2	2	1	2	2	2	1	1	2	1	1	2	2	2	2	1	1

※ LH : 장애발생가능성(Likelihood), IP : 영향(Impact)

※ 리스크 레벨 : 높음(High) : 3, 보통(Moderate) : 2, 낮음(Low) : 1

[표 2]는 [표 1]의 집계를 토대로 모든 평가자들의 정보보호제품 장애발생가능성 및 영향 평균값을 나타낸 것이며, [표 3]은 [표 1]을 토대로 각 평가자별로 품질 리스크를 계산한 결과와 품질 특성별 리스크 평균를 나타낸 것이다.

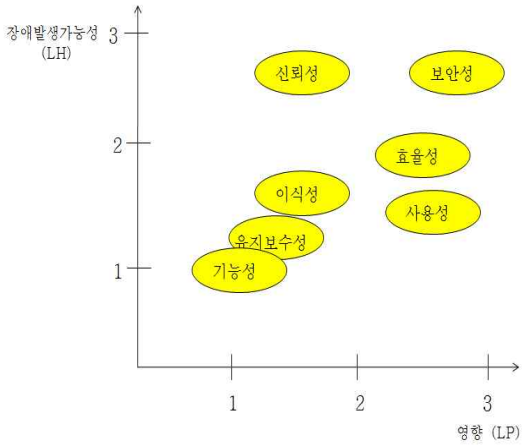
[표 2] 장애발생가능성 및 영향 평균값

구분	장애발생가능성 평균	영향 평균
기능성	1.30	1.40
보안성	2.60	2.90
사용성	1.70	2.60
신뢰성	1.80	2.20
효율성	1.90	2.50
유지보수성	1.40	1.50
이식성	1.70	1.70

[표 3] 평가자별 품질 리스크 계산 결과

설문자	평가자1	평가자2	평가자3	평가자4	평가자5	평가자6	평가자7	평가자8	평가자9	평가자10	품질특성별 리스크 평균
소속	KISA	KISA	KISA	KISA	KISA	KISA	KISA	KISA	KISA	KSEL	
구분	RK	RK	RK	RK	RK	RK	RK	RK	RK	RK	
기능성	2	1	4	2	1	4	1	2	1	1	1.90
보안성	3	9	9	9	6	9	9	9	3	9	7.50
사용성	6	3	3	6	4	3	4	4	6	3	4.20
신뢰성	4	2	2	6	4	6	2	3	6	4	3.90
효율성	2	4	3	9	3	6	1	4	9	9	5.00
유지보수성	2	2	1	4	3	2	1	1	3	1	2.00
이식성	6	4	2	4	2	2	1	4	4	1	3.00

[표 3]에서와 같이 정보보호제품 품질 리스크 설문조사 집계를 토대로 산정된 정보보호제품 품질별 리스크는 보안성이 리스크가 가장 크며, 효율성, 사용성, 신뢰성 순으로 분석되었다. (그림 5)는 [표 2]의 설문조사 결과를 토대로 장애발생가능성과 영향에 따른 정보보호제품 품질 리스크에 대한 분포도이다.



(그림 5) 정보보호제품 품질별 리스크 분포도

4.2 정보보호제품 품질 평가 메트릭 설계

산정된 정보보호제품 품질별 리스크를 토대로 정보보호제품 품질 평가를 위한 메트릭을 설계한다. 정보보호제품의 특정 품질에 대한 리스크가 크면 리스크가 큰 만큼 품질 평가를 위하여 다수의 메트릭을 생성하고, 리스크가 작으면 소수의 메트릭을 생성한다.

4.2.1 품질 평가 메트릭 구성

정보보호제품 품질 평가 메트릭은 다양한 정보보호제품 품질 평가를 위한 메트릭을 생성할 수 있도록 [표 4]와 같이 품질 필수 메트릭, 품질 선택 메트릭, 품질 확장 메트릭으로 정의한다.

[표 4] 품질 평가 메트릭 구성

메트릭 구분	정 의
필수 메트릭	정보보호제품 품질 평가를 위해 정보보호제품의 유형과 무관하게 항상 고정적으로 적용되어야 하는 메트릭
선택 메트릭	정보보호제품 품질 평가를 위해 정보보호제품 유형에 따라 추가적으로 요구되는 메트릭
확장 메트릭	정보보호제품 품질 평가를 위해 품질 평가자가 품질 필수 메트릭과 선택 메트릭에 추가적으로 적용하기 위한 메트릭

4.2.2 리스크 기반 정보보호제품 품질 메트릭

정보보호제품 품질 평가를 위한 리스크 기반 메트릭은 ISO/IEC 9126의 외부 메트릭으로부터 [표 3]의 산정된 정보보호제품 품질별 리스크를 적용하여 [표 5]와 같이 구성한다.

[표 5] 정보보호제품 품질 특성별 리스크 기반 메트릭

품질 특성	제안 방식		ISO/IEC 9126 외부 메트릭수
	필수 메트릭수	선택 메트릭수	
기능성	2	-	11
보안성	20	35	3
사용성	11	-	28
신뢰성	8	-	18
효율성	10	10	26
유지보수성	5	-	16
이식성	6	-	13

ISO/IEC 9126의 외부 메트릭은 보안성 품질에 대하여 3개의 메트릭만을 제공하고 있기 때문에 정보보호제품이 가질 수 있는 보안성에 대한 메트릭을 20개의 필수 메트릭과 35개의 선택 메트릭으로 구성한다. 또한, 효율성 품질에 대하여 26개의 메트릭을 제공하고 있으나 정보보호제품에 공통적으로 적용할 수 있는 10개의 필수 메트릭과 10개의 선택 메트릭으로 설계한다. 보안성과 효율성을 제외한 기능성, 사용성, 신뢰성, 유지보수성, 이식성은 ISO/IEC 9126의 외부 메트릭으로부터 중복되는 메트릭을 배제하고 품질 리스크에 따라 필요한 메트릭만을 선별하여 설계한다.

4.2.3 품질 평가 필수 메트릭

정보보호제품의 품질 평가를 위한 필수 메트릭은 정보보호제품 품질 모델을 바탕으로 [표 6]과 같이 부특성별로 평가 메트릭을 도출하여 총 62개를 정의한다.

정의된 품질 평가 필수 메트릭은 다양한 정보보호제품의 품질 평가를 위해 항상 적용해야 하는 메트릭이다.

[표 6] 정보보호제품 품질 평가 필수 메트릭

특성	부특성	메트릭
기능성	비보안성	비보안성 구현 정확성
	상호운영성	데이터 교환성
보안성	보안감사성	보안경보
		감사데이터 생성
		잠재적인 위반 분석
		보안감사기록 여부에 대한 선택
		감사 증적 저장소 보호
		감사데이터 손실 예측시 대응행동
		감사데이터 손실 방지 행동
	신분확인성	사용자 식별 및 인증
		인증 실패 시 대응행동
		식별 및 인증 데이터의 조합규칙
		인증 피드백 보호
		사용자 세션에 대한 잠금 또는 종료
	보안관리성	보안기능에 대한 관리
		보안속성에 대한 관리
		보안데이터에 대한 관리
		보안데이터 한계치에 대한 관리
		사용자별 보안역할 정의
		장애 시 안전한 상태 유지
	자체보호성	신뢰가능한 타임스탬프
		보안기능 자체 시험

특성	부특성	메트릭
사용성	이해성	기능 이해도
		인터페이스 이해도
		도움말 이해도
		메시지 이해도
	운영성	인터페이스 일관성
		오류 방지성
		오류 복구 용이성
		진행상태 파악 용이성
		운영절차 변경 용이성
	학습성	기능 학습 용이성
	선호도	인터페이스 조정 가능성
신뢰성	성숙성	고장해결율
		결함제거율
	결함허용성	다운회피율
		고장회피율
		백업지원
	회복성	오조작 방지성
		데이터 회복성
		복구가능율
효율성	시간효율성	평균반응율
		반응평균시간
		평균처리율
		처리평균시간
	자원효율성	메모리 최대 사용율
		입·출력장치 자원 사용율
		입·출력 자원사용 대기 평균시간
		CPU 사용율
	전송효율성	데이터전송 효율성
		평균전송속도
유지보수성	분석성	문제 진단 기능 지원율
		문제해결 구현율
	변경성	소프트웨어 변경 제어성
	안정성	환경설정 변경 안정성
	시험성	내장형 시험기능 구현율
이식성	설치성	설치 가능율
		제거 가능율
	호환성	호환율
	지속성	기능 지속가능율
		데이터 지속가능율
	공존성	공존가능율

4.2.4 품질 평가 선택 메트릭

정보보호제품 품질 평가를 위한 필수 메트릭은 다양한 정보보호제품에서 공통적으로 적용될 수 있는 메트릭이다. 그러나, 필수 메트릭만으로는 다양한 정보보호제품의 보안성과 성능적인 품질을 평가하는데 부족하다. 따라서, 선택 메트릭 개념을 도입하여 특정 정보보호제품에서 추가적으로 필요한 보안성 및 효율성을 [표 7]과 같이 정의한다.

[표 7] 정보보호제품 품질 평가 선택 메트릭

특성	부특성	메트릭
보안성	부인방지성	발신 부인방지
		수신 부인방지
	암호지원성	암호키 관리
		암호 연산
	데이터 보호성	접근통제
		데이터 인증
		사용자 데이터의 안전한 유출
		정보흐름통제
		외부로부터 사용자 데이터의 안전한 유입
		제품 부분간 안전한 전송
		잔여정보 보호
		복귀
		저장된 데이터 보호
		신뢰된 제품간 전송되는 사용자데이터 보호
	프라이버시성	익명성, 가명성, 연계불가성, 관찰불가성
	자체보호성	외부전송 보안데이터 보호
		보안데이터 내부전송 보호
		물리적 보호
		안전한 복구
		재사용 공격 탐지
		신뢰된 제품간 전송되는 보안데이터 일관성
		외부 실체 시험
		내부 복제 보안데이터의 일관성
	자원활용성	오류에 대한 내성
		자원사용 우선순위
		자원 할당
	접근성	선택 가능한 보안속성의 범위 제한
		동시 세션 수의 제한
		세션 잠금 및 종료
		제품 접근 경고 및 이력
		제품 세션 설정
	채널안전성	안전한 경로 및 채널

특성	부특성	메트릭
효율성	패킷처리성	패킷처리율
	세션유지성	세션유지율
	부정성	오탐지율(FDR : False Detection Rate)
		타인수락율(FRR : False Rejection Rate)
		본인거부율(FAR : False Accept Rate)
		본인불일치율(FNMR : False Non-Match Rate)
		타인일치율(FMR : False Match Rate)
		동일오류율(EER : Equal Error Rate)
		등록실패율(FTE : Failure To Enroll rate)
		획득실패율(FTA : Failure To Acquire rate)

V. 결론

정보보호제품 사용자가 보안성과 성능을 포함한 좋은 품질의 정보보호제품을 요구하고 있음에도 불구하고 정보보호제품의 품질 평가를 위한 품질 모델 및 메트릭에 대한 연구가 미흡하였다.

이 논문에서는 정보보호제품 품질에 대한 사용자의 요구를 반영하기 위하여 정보보호제품에 대한 품질 특성을 정의하고, 정보보호제품이 제공해야 하는 보안성 및 정보보호제품의 효율성을 평가하기 위한 성능 요소를 분석하였다. 또한, ISO/IEC 9126을 확장하여 정보보호제품의 품질을 평가하기 위한 품질 모델을 7개 주특성과 24개 부특성으로 설계하였다.

정보보호제품에 대한 품질 리스크는 한국인터넷진흥원 등 평가전문가의 설문조사를 통하여 정보보호제품에서 보안성 및 성능에 대한 리스크가 큰 것으로 조사되었다. 이 설문조사 결과를 토대로, 품질 특성별 리스크를 반영하여 항상 공통적으로 적용되어야 하는 필수 메트릭, 정보보호제품별로 확장하여 적용가능한 선택 메트릭, 품질 평가자가 추가할 수 있는 확장 메트릭으로 설계하였으며, 생성된 메트릭은 정보보호제품 품질을 평가하는데 활용될 수 있을 것이다.

참 고 문 헌

[1] Peter G. Neumann, "Computer Related Risks", Addison-Wesley, pp. 231-294, 1995.

[2] H.K.N. Leung, "Quality metrics for intranet applications," Information and management, vol. 38, no. 3, pp. 137-152, Jan. 2001.

[3] M.H. Samadzadeh, K. Nandakumar, "A study of software metrics," The Journal of systems and software, vol. 16, no. 3, pp. 229-234, Nov. 1991.

[4] R. John, "Measures and Techniques for Software Quality Assurance," Computer Science laboratory, Sep. 1991.

[5] 오광근, 김태환, 문전일, 임계영, 김진태, 박수용, "임베디드 시스템 소프트웨어 측정을 위한 품질 특성 연구," 한국정보과학회 추계학술대회발표집, 30(2), pp. 385-387, 2003년 10월.

[6] 장선재, 김행곤, "임베디드 소프트웨어 테스팅 품질에 관한 연구," 한국정보처리학회 춘계학술대회발표집, pp. 176-179, 2007년 5월.

[7] 조재규, 이승종, "소프트웨어 품질향상을 위한 품질 평가 모델에 관한 연구," 한국정보과학회 춘계학술대회발표집, 30(1), pp. 46-48, 2003년 4월.

[8] 박상욱, 정영은, 이원천, 김순용, "패키지 소프트웨어 품질 인증을 위한 시험·평가 프레임워크," 한국정보과학회 추계학술대회발표집, 28(2), pp. 532-534, 2001년 10월.

[9] 양해술, 이하용, 황석형, "산업용 소프트웨어 시험을 위한 품질모델의 개발," 정보처리학회 소프트웨어공학논문지, 8(1), pp. 23-32,

2005년 8월.
[10] 양해술, 이하용, 이정림, 김혁주, "의료용 소프트웨어 품질시험 및 인증체계 구축," 정보처리학회 소프트웨어공학논문지, 8(3), pp. 34-44, 2005년 12월.
[11] 이종민, "보안소프트웨어 제품을 위한 평가 매트릭스 연구," 한국정보과학회 추계학술대회발표집, 33(2), pp. 427-432, 2006년 10월.
[12] 김지혁, 류성열, "응용 오픈소스 소프트웨어 특징에 적합한 논리적 품질 평가 모델에 관한 연구," 정보처리학회논문지D, 16(1), pp. 73-82, 2009년 2월.
[13] ISO/IEC 9126, "Software engineering - Product quality", 2003.
[14] ISO/IEC 14598, "Software Engineering - Product Evaluation", 1999.
[15] ISO/IEC 25000, "SQuaRE : Software product Quality Requirements and Evaluation", 2006.
[16] A.Abran, R.E. Al-Qutaish, J.M. Desharnais and N. Habra, "An Information Model for Software Quality Measurement with ISO Standards," In Proceedings of the International Conference on Software Development(SWDC'2005), Reykjavik, Iceland, pp. 104-116, 2005.
[17] ISO/IEC 15408, "Information Technology - Security techniques - Evaluation criteria for IT security", 2007.9.
[18] Common Criteria Portal, "http://www.commoncriteria portal.org"
[19] 권원일, 박은영, 조현길, "개발자도 알아야 할 소프트웨어 테스팅 실무," pp. 191-200, 소프트웨어 테스팅 연구소, 2006.10.
[20] B. Hickman, D. Newman, S. Tadjudin and T. Martin, "Benchmarking Methodology for Firewall Performance," RFC 3511, Apr. 2003.
[21] 신대철, 심상옥, 김재성, "국내 지문인식시스템 성능시험방법론 연구," 한국정보보호학회 동계학술대회발표집, 12(1), pp. 440-445, 2002년 12월.
[22] 한국정보보호진흥원, 성균관대학교 정보통신공학부, "지문인식시스템 보호프로파일 V2.0," 2008.
[23] 한국정보보호진흥원, 성균관대학교 정보통신공학부, "침입차단시스템 보호프로파일 V2.0," 2008.
[24] 한국정보보호진흥원, 한남대학교 컴퓨터공학과, "침입탐지시스템 보호프로파일 V2.0," 2008.
[25] 한국정보보호진흥원, 한남대학교 컴퓨터공학과, "등급기반 접근통제시스템 보호프로파일 V2.0," 2008.

저 자 소 개

윤여웅

2010년 충북대학교 전자계산학과 이학박사
2000년 10월 ~ 2006년 9월 한국정보보호진흥원 선임연구원
2006년 12월 ~ 2008년 8월 한국시스템보증(주) 이사
2008년 8월 ~ 현재 (주)한국아이티평가원 부사장

<주관심분야 : 정보보호제품 평가, Security Testing, Network Security>

이상호

1989년 숭실대학교 전자계산학과 이학박사
1976년 1월 ~ 1979년 5월 한국전력 전자계산소
1981년 6월 ~ 현재 충북대학교 전기전자컴퓨터공학부 교수

<주관심분야 : Protocol Engineering, Network Security, Network Management, Network Architecture>