情報保護學會論文誌
第19卷 第5號, 2009. 10

정보보호제품 품질평가를 위한 품질 모델 및 메트릭에 관한 연구

윤 여 웅,[1†] 이 상 호[2‡]
[1](주)한국아이티평가원, [2]충북대학교

A Study on the Quality Model and Metrics for Evaluating the Quality of Information Security Products

Yeo-Wung Yun,[1†] Sang-Ho Lee[2‡]
[1]Korea Security Evaluation Laboratory Co., Ltd.,
[2]College of Electrical and Computer Engineering, Chungbuk National University

요 약

정보보호제품 사용자는 보안성과 성능을 포함한 좋은 품질의 정보보호제품을 요구하고 있으나 정보보호제품에 대한 품질평가는 물론 다양한 정보보호제품의 품질을 평가하기 위한 품질 모델과 정보보호제품별 메트릭에 대한 연구가 전무한 실정이다.

본 논문에서는 정보보호제품을 3가지 제품군으로 분류하고, 다양한 정보보호제품이 가질 수 있는 보안성과 성능을 분석하였다. 이를 통하여 정보보호제품의 보안성과 성능이 고려된 품질 모델을 새롭게 정의하였고 정의된 품질모델은 7개의 품질 특성과 24개의 품질 부특성을 가진다. 또한, 정보보호제품의 품질평가에 사용가능한 62개의 공통 메트릭과 45개의 확장 메트릭으로 구성하고 특정 정보보호제품의 품질평가 메트릭을 생성하는 방법을 제안하였다. 제안된 메트릭 생성 방법은 다양한 정보보호제품에 적용할 수 있도록 메트릭의 확장이 가능하며, 침입차단시스템, 침입탐지시스템 및 지문인식시스템에 대한 품질평가 메트릭을 생성하고 검증하여 다양한 정보보호제품에 적용가능함을 보였다.

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 model and metrics for the quality evaluation. In this paper, information security products are categorized into three different types and the security and performance of various information security products are analyzed.

Through this process and after consideration of information security products' security and performance, a new quality model that possesses 7 characteristics and 24 sub-characteristics has been defined. In addition, metrics consisting of 62 common and 45 extended metrics that can be used to evaluate the quality of information security products are introduced, and a proposition for a method of generating the quality evaluation metrics for specific information security products is included. The method of generating metrics proposed in this paper can be extended in order to be applied to a variety of information security products, and by generating and verifying the quality evaluation metrics for firewall, intrusion detection systems and fingerprint systems it is shown that it applicable on a variety of information security products.

Keywords: Information security product, Quality model, Quality evaluation, Quality metrics

접수일(2009년 7월 27일), 게재확정일(2009년 9월 8일)

† 주저자, ywyun@ksel.co.kr
‡ 교신저자, shlee@chungbuk.ac.kr

I. 서 론

2003년 1월 25일 인터넷 대란을 계기로 인터넷 사용자는 정보보호의 중요성을 절실히 인식하게 되었고 이후 다양한 정보보호제품이 널리 보급되어 사용되면서 정보보호제품에 대한 사용자의 요구는 매우 다양해졌다.

초창기 정보보호제품에 대한 사용자의 요구는 보안성에 국한되었다. 사용자는 패킷필터링 및 프록시 기반의 접근통제를 정확히 수행할 수 있는 침입차단시스템과 전송되는 네트워크 패킷을 모두 수집하여 침입행위를 정확히 탐지할 수 있는 침입탐지시스템을 요구했었다. 그러나, 대용량 네트워크 환경으로 전환되면서 사용자들의 요구사항은 매우 다양해졌다. 정보보호제품이 제공해야 하는 보안성은 기본적으로 만족되어야 할 뿐만 아니라 높은 품질을 가진 정보보호제품을 요구하게 되었는데, 요구하는 품질 중에는 보안성 외에도 높은 성능을 요구하고 있다.

품질 평가는 오래전부터 일반 소프트웨어뿐만 아니라 임베디드용 소프트웨어, 패키지용 소프트웨어, 의료용 소프트웨어 등 소프트웨어 품질평가에 대한 연구가 있었고 품질 모델과 메트릭 생성에 대한 많은 성과를 보였다. 그러나, 정보보호제품의 보안성 및 성능 등은 개별적으로 평가가 이루어지고 있으며, 보안성 및 성능 등을 포함한 정보보호제품 품질을 포괄적으로 검증할 수 있는 기준 및 제도가 마련되어 있지 않아 정보보호제품에 대한 품질 평가는 이루어지고 있지 않다. 따라서, 정보보호제품의 사용자가 신뢰하고 사용할 수 있도록 정보보호제품의 품질을 평가하기 위한 모델 및 메트릭에 대한 연구가 필요하다.

본 논문에서는 정보보호제품의 품질평가를 위하여 정보보호제품의 품질 특성을 정의하고, 정보보호제품 품질 모델을 새롭게 정의한다. 정의된 모델로부터 다양한 정보보호제품의 품질을 평가하는데 적용할 수 있는 정형화된 메트릭 생성 방법을 제안하고자 한다. 또한, 제안된 생성 방법으로부터 침입차단시스템, 침입탐지시스템, 지문인식시스템에 대한 품질평가 메트릭을 생성하여 적용가능함을 보였으며, 이는 다양한 정보보호제품의 품질평가 메트릭을 생성하는데 적용가능하다.

II. 관련 제도 및 연구

2.1 소프트웨어 품질평가

소프트웨어 품질은 명시적이고 묵시적인 요구를 만족시키기 위한 능력과 관련된 특성의 총량으로 소프트웨어 품질에 대한 표준은 ISO/IEC JTC1이 국제표준화를 주도하고 있다. ISO/IEC 9126은 소프트웨어 품질 특성과 척도에 관한 지침으로 계층구조로 세분화되어 있으며, 소프트웨어에 관한 품질 특성과 품질 부특성, 메트릭을 정의하고 있다[1,5]. ISO/IEC 14598은 소프트웨어 제품의 품질을 측정하거나 평가하는 절차를 다루고 있으며[2], ISO/IEC 25000(SQuaRE)은 소프트웨어 품질 요구사항 및 평가 프로세스를 크게 5개 부분, 14개 문서로 구성하였다[3].

이러한 소프트웨어 품질 평가는 미국, 유럽 등 주요 선진국을 중심으로 소프트웨어 품질 관련 표준들을 활용하여 소프트웨어 품질을 보증할 수 있는 시험·인증이 수행되어 왔다[8,10]. 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 기능성에 대한 평가를 하였다. 독일의 TuViT은 ISO/IEC 9126, ISO/IEC 14598에 기반을 둔 IT 제품 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 품질평가를 수행하고 있으며, 한국산업기술시험원은 2003년부터 산업용 소프트웨어 표준적합성인증을 실시하였으나 굿소프트웨어 인증으로 통합하여 운영하고 있다.

2.2 정보보호제품 보안성 평가

정보보호제품에 대한 보안성 평가는 ISO/IEC

15408에 정의된 공통평가기준을 기반으로 정보보호 제품의 보안성과 이에 적용된 보증수단이 이러한 요구사항들을 만족하는지에 대한 신뢰도를 확인하는 것으로 전 세계적으로 널리 시행되고 있다[4]. [표 1]에 열거된 정보보호제품 평가기관에서는 공통평가기준을 기반으로 다양한 정보보호제품의 보안성을 평가하고 있다.

[표 1] 전세계 정보보호제품 평가기관

국가	수	주요 평가기관
호주/뉴질랜드	3	CSC, Logica, Stratsec
캐나다	3	CGI Information Systems and Management Consultants Inc., DOMUS IT Security Laboratory, EWA - Canada
프랑스	5	CESTI-AQL - Groupe SILICOMP-AQL, CEA-LETI, CEACI
독일	12	Atos Origin GmbH Prfstelle IT-Sicherheit, ATSEC information security GmbH Prüfstelle für IT-Sicherheit, Brightsight bv IT Security Evaluation Facility, TÜV Informationstechnik GmbH
일본	4	Information Technology Security Center Evaluation Department , Electronic Commerce Security Technology Laboratory Inc.
네델란드	1	Brightsight IT Security Evaluation Facility
노르웨이	3	Aspect Labs, Norconsult ITSEF, Secode Norge AS
스페인	3	del Instituto Nacional de Técnica Aeroespacial(INTA), Applus
스웨덴	2	atsec information security AB, Combitech AB
영국	4	BT, EDS, Logica, SiVenture
미국	9	Arca Common Criteria Testing Laboratory, ATSEC information security corporation, CygnaCom Solutions' Security Evaluation Laboratory, SAIC Common Criteria Testing Laboratory
한국	4	한국인터넷진흥원(KISA), 한국산업기술시험원(KTL), 한국시스템보증(KOSYAS), 한국아이티평가원(KSEL)

2.3 정보보호제품 성능 평가

성능평가는 정보보호제품의 견고성, 효율성 등을 확인하는 것으로 시험의뢰자의 요구에 따라 정보보호 제품의 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/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 다양한 보고서들을 발간하고 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[7].

2.4 기존 연구 문제점 분석

기존 품질평가에 대한 연구는 산업용 소프트웨어, 임베디드 소프트웨어, 의료용 소프트웨어, Open Source 소프트웨어, 보안 소프트웨어, 인트라넷 소프트웨어 등 다양한 소프트웨어 품질에 대한 모델 및 메트릭에 대한 연구가 진행되었다[8-13,15,16,20-23]. [표 2]에서 소프트웨어군별 주요 품질 및 메트릭을 분석하였다.

임베디드 소프트웨어에 대한 품질평가 연구는 소프트웨어 품질을 정의하고, 해당 품질을 평가하기 위한 46개의 평가 메트릭을 정의하였고 패키지 소프트웨어에서는 소프트웨어 품질은 정의되지 않았으나 89개의 평가 메트릭을 정의하였다. 또한, 산업용 소프트웨어에서는 해당 소프트웨어의 품질은 정의되었으나 평가 메트릭은 정의되지 않았고, 의료용 소프트웨어 및

〔표 2〕 소프트웨어군별 품질 모델 및 메트릭

소프트웨어군		임베디드 S/W	패키지 S/W	산업용 S/W	의료용 S/W	Open Source S/W
주요 품질		- 신뢰성 - 이식성 - 실시간성 - 호환성 - 하드웨어 최적화 - 강한 내구성 - 사용성 - 상호운용성	-	- 신뢰성 - 이식성 - 강한 내구성 - 작은 메모리 - 실시간 지원 - 장비 활용성 - 유지보수성 - 유연성	- 신뢰성 - 실시간지원 - 하드웨어와 소프트웨어 부분의 조화 - 강한 내구성 - 사용편의성 - 상호운용성	- 소스공개 - 자발적 참여 - 일찍, 자주 배포 - 대규모 참여자에 의한 개발, 테스트, 디버그 - 커뮤니케이션과 피드백 - 요구사항의 빠른 변화
주요 S/W		- 모니터링 시스템 - 교통관제 - 엘리베이터 시스템 - 가전제품 - 휴대용전화기	교육용 소프트웨어	- CAD/CAM /CAE용 소프트웨어 - 공정제어용 소프트웨어 - EC 소프트웨어	-	- eMule - Azureus - Ares Galaxy - 7-Zip - FileZilla
평가 항목	주특성	6개	7개	-	6개	6개
	부특성	20개	-	-	27개	12개
	메트릭	46개	89개	-	85개	12개

Open Source 소프트웨어에서는 해당 소프트웨어에 대한 품질과 평가 메트릭이 정의되었으며, Open Source에 대한 품질평가 메트릭에는 성능, 보안, 지원 등에 대한 특성은 배제되었다.

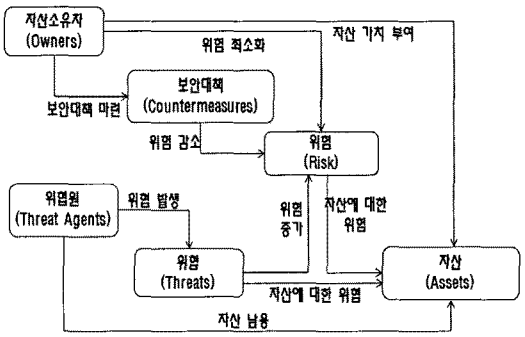
그러나, 이러한 기존 연구는 특정 소프트웨어군에 종속되어 특정 소프트웨어군에 다양한 소프트웨어가 존재하는 것이 고려되지 못했고, 유연한 메트릭을 제공하지 못하고 고정된 메트릭을 생성하여 사용하였다. 이는 특정 소프트웨어군의 다양한 소프트웨어의 품질을 평가하는데 한계가 있으며, 기존 연구 결과를 보안성과 성능이 중요한 다양한 정보보호제품의 품질을 평가하기 위한 메트릭으로 활용하는 것은 적용불가능하다.

III. 정보보호제품 품질 모델 정의

기존 품질평가에 대한 연구결과를 정보보호제품의 품질을 평가하는데 적용할 수 없기 때문에 정보보호제품에 대한 품질 특성을 정의하고, 정보보호제품이 제공해야 하는 보안성 및 정보보호제품의 효율성을 평가하기 위한 성능 요소를 분석하였다. 이를 통하여 정보보호제품에 대한 품질 모델을 새롭게 정의한다.

3.1 정보보호제품 특성

자산소유자는 〔그림 1〕과 같이 위협원으로부터 발생되는 위협들로부터 운영환경 내의 자산을 보호하기 위하여 자산의 가치를 부여하고 위험을 감소시키기 위해 다양한 보안대책을 마련하며, 보안대책은 다양한 정보보호제품으로 구현된다[4].



〔그림 1〕 정보보호 개념도

정보보호제품은 앞서 살펴본 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.

■ 안전한 자산 보호 기능

정보보호제품은 운영환경 내의 자산을 안전하게 보호하기 위하여 다양한 보안성을 제공하며, 정보보호제품이 제공하는 보안성은 〔표 3〕과 같이 공통평가기준의 보안기능요구사항을 기반으로 11가지로 구분하였고, 세부적인 보안성을 55가지로 정의하였다[4]. 다

〔표 3〕 정보보호제품 보안성

구분	기능수	세부 보안성
보안감사성	7	보안감사 자동대응, 보안감사 데이터 생성, 보안감사 분석, 보안감사 검토, 보안감사 사건 선택, 보안감사 사건 저장, 감사데이터 손실 방지
부인방지성	2	발신 부인방지, 수신 부인방지
암호지원성	2	암호키 관리, 암호 연산
데이터보호성	10	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 사용자 데이터 보호
신분확인성	5	인증 실패, 비밀정보의 검증 및 생성, 사용자 인증, 사용자 식별, 사용자-주체 연결
보안관리성	5	보안 기능 관리, 보안 속성 관리, 보안데이터 관리, 폐지, 사용자 보안역할 관리
프라이버시성	4	익명성, 가명성, 연계불가성, 관찰불가성
자체보호성	11	안전한 상태 유지, 외부전송 보안데이터 보호, 보안데이터 내부전송 보호, 물리적 보호, 안전한 복구, 재사용 공격 탐지, 신뢰가능한 타임스탬프 제공, 신뢰된 제품간 전송되는 보안데이터 일관성, 외부 실체 시험, 내부 복제 보안데이터 일관성, 보안기능 자체 시험
자원활용성	3	오류에 대한 내성, 자원사용 우선순위, 자원 할당
접근성	5	선택 가능한 보안속성의 범위 제한, 동시 세션 수의 제한, 세션 잠금 및 종료, 제품 접근 경고 및 이력, 제품 세션 설정
채널 안전성	1	안전한 채널 및 경로

양한 정보보호제품에서 제공되는 정의된 보안성은 품질평가 시 보안성이 정확하게 제공되는지 필히 확인되어야 한다.

■ 높은 성능

정보보호제품은 효율성을 평가하기 위해서 매우 다양한 성능 요소가 적용가능하며, 일반 소프트웨어는 필요할 때 구동시켜서 사용하지만 정보보호제품은 운영환경 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 있으며, 지연은 전송지연, 전파지연, 처리지연, 대기지연 등으로 구분될 수 있다〔6〕. 지문인식시스템의 경우도 타인수락율, 본인거부율, 어미지 등록 및 획득 시 실패한 비율, 특정점 추출 및 비교에 걸리는 시간 등을 제시하고 있다〔7〕.

■ 사용편의성

정보보호제품의 사용자는 한 조직의 정보보호담당자처럼 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.

■ 신뢰성

정보보호제품은 항상 동작되는 것은 보장하기 위하여 정보보호제품 사용 시 제품을 다운시키는 결함이나 심각한 고장을 발생시키는 결함에 대해 자체적인 대응능력을 가져야 하며, 사용자의 오조작으로 인해 발생할 수 있는 심각한 오류를 사전에 방지할 수 있도록 대응할 수 있어야 한다.

■ 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 운영환경 내 자산의 보호를 보장할 수 없을 것이다.

■ 통합 호환성

정보보호제품은 설치 및 제거 절차에 따라 정보보

호제품을 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.

3.2 정보보호제품 분류

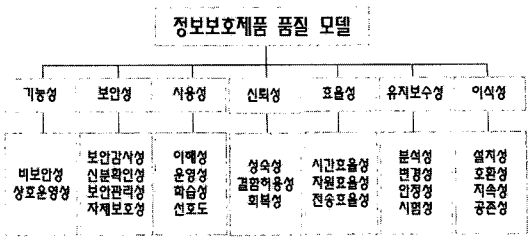
정보보호제품은 국가나 사용 환경 등에 따라 다양하게 분류할 수 있으나, [표 4]와 같이 네트워크 정보보호제품군, 정보보호 기반 제품군, 컴퓨팅 정보보호제품군으로 정보보호제품을 분류하였으며, 각 정보보호제품은 다양한 보안성을 제공한다[17-19].

3.3 정보보호제품 품질 모델

정보보호제품의 품질 모델은 일반 소프트웨어와 달리 보안성과 성능에 대한 품질이 매우 중요하기 때문

[표 4] 정보보호제품 분류

제품군	유형	주요 제품
네트워크 정보보호제품군	네트워크 기반	- 라우터, 스위치, 게이트웨이 - 무선랜, 이동통신보안, 웹보안 - 침입탐지시스템, 침입방지시스템, 트래픽관리장치
	네트워크간	- 침입차단시스템, 가상사설망, 네트워크접근제어제품 - SSO, EAM, VoIP
정보보호 기반 제품군	보안 관리	- 안티바이러스, 취약점 점검도구 - 불건전정보차단도구, ESM - 위험분석도구, DRM
	생체 인식	- 지문, 얼굴, 홍채, 정맥, 서명
	스마트카드	- 칩, 카드운영체제, 판독기, 응용제품
	인증 솔루션	- CA, RA, 권한관리기반(PMI), OCSP, SCVP
컴퓨팅 정보보호제품군	서버 보안	- 리눅스, 유닉스, 윈도우 기반 운영체제
	데이터 베이스	- 관계형 등 DB, DB 보안
	메일 보안	- SMIME, PGP
	디바이스 보안	- 복합기 보안
	PC 보안	- PC 접근통제, 키보드 보안, 보안 USB



[그림 2] 정보보호제품 품질 모델

에 3.1에서 정의된 다양한 정보보호제품의 품질로부터 ISO/IEC 9126 기반으로 [그림 2]와 같이 7개의 주특성과 24개의 부특성으로 정의하였다.

기능성은 정보보호제품이 제공하는 보안성 외의 비보안성의 구현이 정확한지와 다른 제품과 상호작용을 하는 기능이 정상적으로 동작하는지를 평가한다. 보안성은 정보보호제품이 제공해야 할 공통적으로 제공하는 최소한의 보안성을 도출하여 부특성으로 정의한다. 보안성의 부특성은 다양한 정보보호제품에서 공통적으로 제공되어야 하는 최소한의 보안성으로써 [표 4]에 포함된 네트워크 정보보호제품군인 침입차단시스템과 침입탐지시스템, 정보보호 기반 제품군인 지문인식시스템, 컴퓨팅 정보보호제품군인 운영체제보안시스템의 보안기능을 분석하여 정보보호제품이 공통적으로 제공해야 하는 보안성을 보안감사성, 신분확인성, 보안군인성, 자체보호성으로 정의하였다[24-27]. 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, 적은 자원(메모리/디스크/CPU/입출력장치 등) 사용으로 자원의 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.

IV. 품질평가 메트릭 생성방법 설계

본 절에서는 3장에서 정의된 품질 모델을 통하여 다양한 정보보호제품에 적용가능한 품질평가 메트릭을 생성하는 방법을 제안한다. 기존 연구는 소프트웨어군별로 고정된 메트릭을 제안하였지만 본 논문에서는 다양한 정보보호제품에 유연하게 적용할 수 있도록 항상 고정적으로 적용되어야 하는 공통 메트릭과 정보보호제품별로 추가적으로 적용가능한 확장 메트릭으로 구분하여 적용하였다.

4.1 품질평가 공통 메트릭

정보보호제품의 품질평가를 위한 공통 메트릭은 3.3에서 서술된 정보보호제품 품질 모델을 바탕으로 〔표 5〕와 같이 부특성별로 평가 메트릭을 도출하여 총 62개를 정의하였다. 정의된 공통 메트릭은 다양한 정보보호제품의 품질평가를 위해 항상 적용해야 하는 메트릭이며, 메트릭 측정 유형은 만족여부(Pass), 비율(Scale), 숫자(Number), 시간(Time)으로 정의하였다.

만족여부는 보안성이 만족되지 않으면 정보보호제품이 보호해야 하는 자산이 취약할 수 있기 때문에 항상 정상동작되어야 하는 부분에 적용될 수 있는 항목이고, 비율은 품질에 가장 많이 영향을 주는 요소로써 백분율로 표현된다. 숫자는 해당 메트릭에 대해 정량적으로 평가할 수 있는 것을 의미하며, 시간을 측정하는 메트릭은 시간으로 표현한다.

〔표 5〕 정보보호제품 품질평가 공통 메트릭

특성	부특성	메트릭	측정유형
기능성	비보안성	비보안성 구현 정확성	비율
	상호운영성	데이터 교환성	
보안성	보안감사성	보안경보 기능	만족여부
		감사데이터 생성 기능	
		잠재적인 위반 분석 기능	
		보안감사기록 여부에 대한 선택 기능	
		감사 증적 저장소 보호 기능	
		감사데이터 손실 예측시 대응행동	
		감사데이터 손실 방지를 위한 기능	
	신분확인성	사용자 식별 및 인증 기능 제공	만족여부
		인증 실패 시 대응행동 제공	
		식별 및 인증 데이터의 조합규칙 제공	
		인증 피드백 보호 기능	
		사용자 세션에 대한 잠금 또는 종료 기능	
	보안관리성	보안기능에 대한 관리	만족여부
		보안속성에 대한 관리	
		보안데이터에 대한 관리	
		보안데이터 한계치에 대한 관리	
		사용자별 보안역할 정의	
	자체보호성	장애 시 안전한 상태 유지	만족여부
		신뢰가능한 타임스탬프 제공	
		보안기능 자체 시험	
사용성	이해성	기능 이해도	비율
		인터페이스 이해도	
		도움말 이해도	
		메시지 이해도	
	운영성	인터페이스 일관성	비율
		오류 방지성	
		오류 복구 용이성	
		진행상태 파악 용이성	
		운영절차 변경 용이성	
	학습성	기능 학습 용이성	비율
	선호도	인터페이스 조정 가능성	비율
신뢰성	성숙성	고장해결율	비율
		결함제거율	
	결함허용성	다운회피율	비율
		고장회피율	
		백업지원 기능	만족여부
	회복성	오조작 방지성	비율
		데이터 회복성	
		복구성	
효율성	시간효율성	평균반응율	비율
		반응평균시간	시간
		평균처리율	비율
		처리평균시간	시간
	자원효율성	디스크 및 메모리 사용율	비율
		입·출력장치 자원 사용율	
		입·출력 자원사용 대기평균시간	시간
		CPU 사용율	비율
	전송효율성	데이터전송 효율성	비율
		평균전송속도	숫자
유지보수성	분석성	문제 진단/분석 기능 지원율	비율
		문제해결 구현율	
	변경성	환경설정 변경 가능율	비율
	안정성	환경설정 변경 성공율	비율
	시험성	내장형 시험기능 구현율	비율
이식성	설치성	설치 가능율	비율
		제거 가능율	
	호환성	호환율	비율
	지속성	기능 지속가능율	비율
		데이터 지속가능율	
	공존성	공존가능율	비율

4.2 품질평가 확장 메트릭

4.2에 서술된 정보보호제품 품질평가를 위한 공통 메트릭은 다양한 정보보호제품에서 공통적으로 적용될 수 있는 메트릭이다. 그러나, 공통 메트릭만으로는 다양한 정보보호제품의 보안성과 성능적인 품질을 평가하는데 부족하다. 따라서, 확장 메트릭 개념을 도입하여 특정 정보보호제품에서 추가적으로 필요한 보안성 및 성능을 〔표 6〕과 같이 45개로 정의한다. 정의된 확장 메트릭은 다양한 정보보호제품의 추가적인 보안성과 성능을 품질평가에 적용되어 보다 정확한 품질평가를 할 수 있다.

〔표 6〕 정보보호제품 품질평가 확장 메트릭

특성	부특성	메트릭	측정유형
보안성	부인방지성	발신 부인방지 기능	만족여부
		수신 부인방지 기능	
	암호지원성	암호키 관리 기능	만족여부
		암호 연산 기능	
	데이터보호성	접근통제 기능	만족여부
		데이터 인증 기능	
		사용자 데이터의 안전한 유출 기능	
		정보흐름통제 기능	
		외부로부터 사용자 데이터의 안전한 유입	
		제품 부분간 안전한 전송 기능	
		잔여정보 보호 기능	
		복귀 기능	
		저장된 데이터 보호 기능	
		신뢰된 제품간 전송되는 사용자 데이터 보호	
	프라이버시성	익명성, 가명성, 연계불가성, 관찰불가성	만족여부
	자체보호성	외부전송 보안데이터 보호 기능	만족여부
		보안데이터 내부전송 보호 기능	
		물리적 보호 기능	
		안전한 복구 기능	
		재사용 공격 탐지 기능	
		신뢰된 제품간 전송되는 보안데이터 일관성	
		외부 실체 시험	
		내부 복제 보안데이터의 일관성	
	자원활용성	오류에 대한 내성 기능	만족여부
		자원사용 우선순위 기능	
		자원 할당 기능	
	접근성	선택 가능한 보안속성의 범위 제한 기능	만족여부
		동시 세션 수의 제한 기능	
		세션 잠금 및 종료 기능	
		제품 접근 경고 및 이력 기능	
		제품 세션 설정 기능	
	채널안전성	안전한 경로 및 채널 기능	만족여부
효율성	패킷처리성	패킷처리율	비율
	세션유지성	세션유지율	비율
	부정성	오탐지율 (FDR : False Detection Rate)	비율
		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)	

4.3 정형화된 메트릭 생성 방법

정보보호제품의 품질평가를 위해 품질평가 메트릭을 생성하는 정형화된 방법은 특정 정보보호제품이 가질 수 있는 보안성 및 성능이 매우 다양하기 때문에 앞서 정의된 공통 메트릭과 확장 메트릭을 이용한다. 정형화된 메트릭 생성방법은 전체적으로 아래와 같이 3단계로 구성된다. 특정 정보보호제품의 품질평가를 위한 메트릭을 생성하기 위해서는 제안된 정형화된 품질평가 메트릭 생성방법을 통하여 생성할 수 있으며, 다양한 정보보호제품에 적용가능하다.

■ *단계 1 : 공통 메트릭 적용*

특정 정보보호제품의 정형화된 품질평가 메트릭을 생성하기 위하여 〔표 5〕의 정보보호제품 품질평가를 위한 공통 메트릭을 모두 수용하여 기본적으로 최소 62개의 품질평가 메트릭을 생성.

■ *단계 2 : 확장 메트릭 적용*

단계 1에서 구성된 62개의 품질평가 메트릭에 〔표 6〕의 정보보호제품 품질평가를 위한 확장 메트릭으로부터 특정 정보보호제품의 품질평가를 위해 필요한 보안성 및 성능을 추가하여 품질평가 메트릭을 생성.

■ *단계 3 : 추가 메트릭 생성*

단계 1과 단계 2로부터 구성된 품질평가 메트릭에는 언급되지 않았지만 품질평가자가 해당 정보보호제품의 품질평가를 위해 추가적으로 요구되는 보안성 및 성능을 추가하여 전체 품질평가 메트릭을 생성.

V. 제안된 메트릭 생성방법 적용 및 검증

4장에서 정의된 정보보호제품 품질평가를 위한 공통 메트릭과 확장 메트릭으로부터 제안된 다양한 정보보호제품의 품질평가를 위한 정형화된 메트릭 생성 방법으로부터 〔표 4〕의 주요 정보보호제품인 침입차단시스템, 침입탐지시스템, 지문인식시스템에 대한 품질평가 메트릭을 생성하고 그 적절성을 검증한다.

5.1 침입차단시스템

침입차단시스템은 보호하고자 하는 네트워크에 대한 서비스 요청을 통제하여 허가되지 않은 접근을 차단하는 것으로, 침입차단시스템의 품질을 평가하기 위한 메트릭은 제안된 정형화된 메트릭 생성방법에 따라 아래와 같이 생성한다.

단계1	62개 공통 메트릭으로 구성		
단계2	보안성	데이터 보호성	접근통제 기능
			정보흐름통제 기능
		접근성	세션 잠금 및 종료 기능
	효율성	패킷처리성	패킷처리율
		세션유지성	세션유지율
단계3	없음		

침입차단시스템의 품질평가를 위하여 제안된 방법을 통하여 생성된 메트릭은 총 67개로 구성된다. 품질평가자는 〔표 5〕로부터 62개의 공통 메트릭을 생성하고, 〔표 6〕으로부터 추가적으로 필요한 보안성의 부특성인 데이터보호성과 접근성에 대한 3개와 효율성의 패킷처리성과 세션유지성에 대한 2개의 품질평가 메트릭을 생성한다. 또한, 〔표 5〕와 〔표 6〕에는 정의되지 않았으나 침입차단시스템의 품질평가를 위하여 필요한 추가적인 품질평가 메트릭은 없다.

5.2 침입탐지시스템

침입탐지시스템은 보호대상 자산의 사용자 활동에 대한 데이터를 수집·분석하여 불법적인 사건을 실시간으로 탐지하며, 분석된 결과에 따라 시스템을 보호하기 위하여 대응기능을 수행하는 것으로, 침입탐지시스템의 품질을 평가하기 위한 메트릭은 제안된 정형화된 메트릭 생성방법에 따라 아래와 같이 생성한다.

단계1	62개 공통 메트릭으로 구성		
단계2	효율성	패킷처리성	패킷처리율
		부정성	오탐지율 (FDR : False Detection Rate)
단계3	보안성	침입탐지성	침입탐지 대상사건에 대한 정보 수집
			침입에 대한 분석 및 탐지 기능
			침입탐지 시 대응 기능
			새로운 탐지규칙 갱신 기능

침입탐지시스템 품질평가를 위하여 제안된 방법을 통하여 생성된 메트릭은 총 68개로 구성된다. 품질평가자는 〔표 5〕로부터 62개의 공통 메트릭을 생성하고, 〔표 6〕으로부터 추가적으로 필요한 효율성의 부특성인 패킷처리성과 부정성에 대한 2개의 품질평가 메트릭을 생성한다. 단계 3에서는 〔표 5〕와 〔표 6〕에는 정의되지 않았으나 침입탐지시스템의 품질평가를 위해 필요한 품질평가 메트릭을 보안성의 부특성인 침입탐지성을 정의하여 추가적으로 4개의 메트릭을 생성하였다.

5.3 지문인식시스템

지문인식시스템은 사용자가 제공한 신원주장 식별자를 식별한 후 이를 기반으로 사용자가 제공한 지문정보와 해당 사용자의 등록된 지문정보를 비교하여 정합여부를 결정함으로써 사용자 신원을 인증하는 것으

단계1	62개 공통 메트릭으로 구성		
단계2	보안성	데이터 보호성	잔여정보 보호 기능
	효율성	부정성	타인수락율(FRR)
			본인거부율(FAR)
			본인불일치율(FNMR)
			타인일치율(FMR)
			동일오류율(EER)
			등록실패율(FTE)
			획득실패율(FTA)
단계3	보안성	신분 확인성	사용자에 대한 BIR(Biometric Information Record) 생성 기능

로, 지문인식시스템의 품질을 평가하기 위한 메트릭은 제안된 정형화된 메트릭 생성방법에 따라 아래와 같이 생성한다.

지문인식시스템 품질평가를 위하여 제안된 방법을 통하여 생성된 메트릭은 총 71개로 구성된다. 품질평가자는 〔표 5〕로부터 62개의 공통 메트릭을 생성하고, 〔표 6〕으로부터 추가적으로 필요한 보안성의 부특성인 데이터보호성에 대한 1개와 효율성의 부특성인 패킷처리성과 부정성에 대한 7개의 품질평가 메트릭을 생성한다. 단계 3에서는 〔표 5〕와 〔표 6〕에는 정의되지 않았으나 지문인식시스템의 품질평가를 위해 필요한 품질평가 메트릭을 보안성의 부특성인 신분확인성에 대해 추가적으로 1개의 메트릭을 생성하였다.

5.4 제안 방법 적정성 검증

정보보호제품에 대해 제안된 정형화된 생성방법을 통하여 생성된 품질평가 메트릭은 2가지 방법을 통하여 메트릭의 적정성을 검증하고자 한다.

〔방법 1〕 *품질 모델 비교를 통한 검증*

품질평가 메트릭은 정의된 품질 모델을 기반으로 생성되기 때문에 품질 모델이 적정하다면 해당 품질 모델을 통해 생성된 메트릭도 적정할 것이며, 생성된 메트릭이 소프트웨어 품질 특성과 척도를 정의한 ISO/IEC 9126과의 비교·분석하여 적정성 여부를 확인한다.

〔표 7〕은 제안된 품질 모델이 ISO/IEC 9126의 품질 기준을 만족하는지를 확인하기 위하여 비교·분석하였다. ISO/IEC 9126에서 반영되지 않은 기능

〔표 7〕 제안된 방법과 ISO/IEC 9126간 품질 비교

ISO/IEC 9126		제안된 품질 모델	
특성	부특성	특성	부특성
기능성	적합성	기능성	비보안성
		보안성	보안감사성 신분확인성 보안관리성 자체보호성
	정확성	기능성	비보안성
	상호운용성	기능성	상호운영성
	보안성	보안성	보안감사성 신분확인성 보안관리성 자체보호성
신뢰성	성숙성	신뢰성	성숙성
	결함허용성	신뢰성	결함허용성
	회복성	신뢰성	회복성
사용성	이해성	사용성	이해성
	학습성	사용성	학습성
	운영성	사용성	운영성
	선호도	사용성	선호도
효율성	시간행위	효율성	시간효율성
	자원효율	효율성	자원효율성 전송효율성
유지보수성	분석성	유지보수성	분석성
	변경성	유지보수성	변경성
	안정성	유지보수성	안정성
	시험성	유지보수성	시험성
이식성	적응성	이식성	호환성
	설치성	이식성	설치성
	공존성	이식성	공존성
	대체성	이식성	지속성

〔표 8〕 침입차단시스템의 생성된 메트릭과 보안기능요구사항 비교

침입차단시스템 보호프로파일		보안성 품질평가 메트릭	
보안기능 클래스	보안기능 컴포넌트	부특성	메트릭
보안 감사	FAU_ARP.1 FAU_GEN.1 FAU_SAA.1 FAU_SAR.1 FAU_SAR.3 FAU_SEL.1 FAU_STG.1 FAU_STG.3 FAU_STG.4	보안 감사성	보안경보 기능
			감사데이터 생성 기능
			잠재적인 위반 분석 기능
			보안감사기록 여부에 대한 선택 기능
			감사 증적 저장소 보호 기능
			감사데이터 손실 예측시 대응행동
			감사데이터 손실 방지를 위한 기능
사용자 데이터 보호	FDP_IFC.2 FDP_IFF.1	데이터 보호성	접근통제 기능
			정보흐름통제 기능
식별 및 인증	FIA_AFL.1 FIA_ATD.1 FIA_SOS.1 FIA_UAU.1 FIA_UAU.4 FIA_UAU.7 FIA_UID.2	신분 확인성	사용자 식별 및 인증 기능 제공
			인증 실패 시 대응행동 제공
			식별 및 인증 데이터의 조합규칙 제공
			인증 피드백 보호 기능
			사용자 세션에 대한 잠금 또는 종료 기능
보안 관리	FMT_MOF.1 FMT_MSA.1 FMT_MSA.3 FMT_MTD.1 FMT_MTD.2 FMT_SMF.1 FMT_SMR.1	보안 관리성	보안기능에 대한 관리
			보안속성에 대한 관리
			보안데이터에 대한 관리
			보안데이터 한계치에 대한 관리
			사용자별 보안역할 정의
TSF 보호	FPT_TST.1	자체 보호성	장애 시 안전한 상태 유지
			신뢰가능한 타임스탬프 제공
			보안기능 자체 시험
TOE 접근	FTA_SSL.1 FTA_SSL.3	접근성	세션 잠금 및 종료 기능

성의 적합성은 정보보호제품의 제공하는 기능이 사용자의 요구사항에 얼마나 적합한지를 평가하는 것으로써 제안된 품질 모델의 기능성의 비보안성과 보안성이 해당 특성을 만족시킨다. 따라서, 제안된 품질 모델은 정보보호제품 품질 평가를 위해 적정하며, 해당 품질 모델을 통해 제안된 정형화된 메트릭 생성 방법은 적정하다.

〔방법 2〕 *최소 보안성 비교를 통한 검증*

품질평가 메트릭은 정보보호제품별 최소한으로 제공해야 할 보안성을 포함해야 하므로 생성된 메트릭이 각 정보보호제품별로 최소한의 보안기능요구사항을 정의한 보호프로파일과의 비교·분석을 통하여 적정성 여부를 확인한다.

5.1에서 제안된 생성 방법을 통하여 생성된 침입차단시스템 품질평가를 위한 보안성에 대한 메트릭이 최소 보안성을 정의하고 있는 침입차단시스템 보호프로파일의 보안기능요구사항과 비교분석하여 생성방법의 적정성을 확인한다. 〔표 8〕에서 보시는 바와 같이 4.3에서 설계된 정형화된 방법을 통하여 생성된 침입차단시스템의 보안성 품질평가 메트릭은 침입차단시스템 보호프로파일에서 요구하는 보안기능요구사항들을 만족시킨다. 따라서, 제안된 생성 방법은 정보보호제품 품질 평가를 위한 메트릭 생성 방법으로 적정하다.

VI. 결 론

본 논문에서는 정보보호제품 사용자가 보안성과 성능을 포함한 좋은 품질의 정보보호제품을 요구하고 있음에도 불구하고 기존 품질평가에 대한 연구결과를 정보보호제품의 품질평가에 적용할 수 없기 때문에 정보보호제품에 대한 품질 특성을 정의하고, 정보보호제품이 제공해야 하는 보안성 및 정보보호제품의 효율성을 평가하기 위한 성능 요소를 분석하였다. 이를 통하여 보안성과 성능이 고려된 정보보호제품의 품질을 평가하기 위한 품질 모델을 새롭게 정의하였고, 다양한 정보보호제품에 유연하게 적용할 수 있도록 항상 고정적으로 적용되어야 하는 공통 메트릭과 정보보호제품별로 추가적으로 적용가능한 확장 메트릭으로 구분하여 메트릭을 정의하였다.

또한, 정의된 정보보호제품 품질평가를 위한 공통 메트릭과 확장 메트릭으로부터 제안된 다양한 정보보호제품의 품질평가를 위한 정형화된 메트릭 생성 방법으로부터 침입차단시스템, 침입탐지시스템, 지문인식시스템에 대한 품질평가 메트릭을 생성하고 ISO/IEC 9126의 품질모델 및 정보보호제품 보호프로파일과의 비교·분석을 통하여 생성방법에 대한 적정성을 검증하였다.

따라서, 제안된 정형화된 메트릭 생성 방법은 다양한 정보보호제품을 수용할 수 있도록 메트릭의 확장이 가능하기 때문에 각 정보보호제품의 품질을 평가하는데 제안된 품질평가 메트릭 생성 방법을 통하여 원하는 메트릭을 생성하여 품질평가에 적용할 수 있을 것이다.

참 고 문 헌

〔1〕 ISO/IEC 9126, "Software engineering - Product quality," 2003.

〔2〕 ISO/IEC 14598, "Software Engineering - Product Evaluation," 1999.

〔3〕 ISO/IEC 25000, "SQuaRE : Software product Quality Requirements and Evaluation," 2006.

〔4〕 ISO/IEC 15408, "Information Technology - Security techniques - Evaluation criteria for IT security," 2006.

〔5〕 IEEE Std 1061-1998, "IEEE Standard for a Software Quality Metrics Methodology," 1998.

〔6〕 B. Hickman, D. Newman, S. Tadjudin, and T. Martin, "Benchmarking Methodology for Firewall Performance," RFC 3511, Apr. 2003.

〔7〕 신대철, 심상옥, 김재성, "국내 지문인식시스템 성능시험방법론 연구," 한국정보보호학회 동계학술대회발표집, pp. 440-445, 2002년 12월.

〔8〕 오광근, 김태환, 문전일, 임계영, 김진태, 박수용, "임베디드 시스템 소프트웨어 측정을 위한 품질 특성 연구," 한국정보과학회 추계학술대회발표집, pp. 385-387, 2003년 10월.

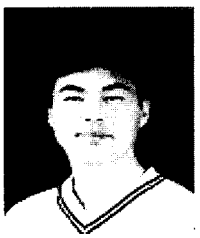
〔9〕 장선재, 김행곤, "임베디드 소프트웨어 테스팅 품질에 관한 연구," 한국정보처리학회 춘계학술대회발표집, pp. 176-179, 2007년 5월.

〔10〕 조재규, 이승종, "소프트웨어 품질향상을 위한 품질평가 모델에 관한 연구," 한국정보과학회 춘계학술대회발표집, pp. 46-48, 2003년 4월.

〔11〕 박상욱, 정영은, 이원천, 김순용, "패키지 소프트웨

어 품질 인증을 위한 시험·평가 프레임워크," 한국정보과학회 추계학술대회발표집, pp. 532-534, 2001년 10월.
[12] H.K.N. Leung, "Quality metrics for intranet applications," Information and management, vol. 38, no. 3, pp. 137-152, Jan. 2001.
[13] M.H. Samadzadeh and K. Nandakumar, "A study of software metrics," The Journal of systems and software, vol. 16, no. 3, pp. 229-234, Nov. 1991.
[14] Linda and Westfall, "A Practical Process to Establish Software Metrics," Software quality professional, vol. 8, no. 2, pp. 11-22, Mar. 2006.
[15] A. Griman, M. Perez, L. Mendoza, and F. Losavio, "Feature analysis for architectural evaluation methods," The Journal of systems and software, vol. 79, no. 6, pp. 871-888, June 2006.
[16] R. John, "Measures and Techniques for Software Quality Assurance," Computer Science laboratory, Sep. 1991.
[17] 오흥룡, 염흥열, "국제 공통평가기준(CC) 체제하에 평가된 정보보호제품 분석," 정보보호학회지, 14(4), pp. 54-67, 2004년 8월.
[18] 최승, 최상수, 이강수, "CC기반 통합제품 평가업무량 모델과 정보보호제품 분류체계," 한국정보과학회 춘계학술대회발표집, pp. 328-330, 2004년 4월.
[19] 국가정보원, "정보보호제품 평가인증 수행규정," 2009년 3월.
[20] 양해술, 이하용, 황석형, "산업용 소프트웨어 시험을 위한 품질모델의 개발," 정보처리학회 소프트웨어공학논문지, 8(1), pp. 23-32, 2005년 8월.
[21] 양해술, 이하용, 이정림, 김혁주, "의료용 소프트웨어 품질시험 및 인증체계 구축," 정보처리학회 소프트웨어공학논문지, 8(3), pp. 34-44, 2005년 12월.
[22] 이종민, "보안소프트웨어 제품을 위한 평가 매트릭스 연구," 한국정보과학회 추계학술대회발표집, pp. 427-432, 2006년 10월.
[23] 김지혁, 류성열, "응용 오픈소스 소프트웨어 특징에 적합한 논리적 품질 평가 모델에 관한 연구," 정보처리학회논문지D, 16(1), pp. 73-82, 2009년 2월.
[24] 한국정보보호진흥원, 성균관대학교 정보통신공학부, "침입차단시스템 보호프로파일 V2.0," 2008.
[25] 한국정보보호진흥원, 한남대학교 컴퓨터공학과, "침입탐지시스템 보호프로파일 V2.0," 2008.
[26] 한국정보보호진흥원, 성균관대학교 정보통신공학부, "지문인식시스템 보호프로파일 V2.0," 2008.
[27] 한국정보보호진흥원, 한남대학교 컴퓨터공학과, "등급기반 접근통제시스템 보호프로파일 V2.0," 2008.

〈著者紹介〉



윤 여 웅 (Yeo-Wung Yun) 종신회원
1996년 2월: 한남대학교 컴퓨터공학과 학사
1998년 2월: 한남대학교 컴퓨터공학과 석사
2000년 10월 ~ 2006년 9월: 한국정보보호진흥원 선임연구원
2006년 12월 ~ 2008년 8월: 한국시스템보증(주) 이사
2008년 8월 ~ 현재: (주)한국아이티평가원 부사장
〈관심분야〉 정보보호제품 평가, Security Testing, Network Security

이 상 호 (Sang-Ho Lee) 정회원
1976년 2월: 숭실대학교 전자계산학과 학사
1981년 2월: 숭실대학교 전자계산학과 석사
1989년 2월: 숭실대학교 전자계산학과 박사
1981년 3월 ~ 현재: 충북대학교 전기전자컴퓨터공학부 교수
〈관심분야〉 네트워크 보안, Protocol Engineering, Network Management