한국산학기술학회논문지
Vol. 11, No. 12 pp. 5058-5071, 2010

침입차단시스템의 품질평가 방법

이하용[1*], 권원일[2], 양해술[3]
[1]서울벤처정보대학원대학교 정보관리학과
[2](주)STA컨설팅, [3]호서대학교 벤처전문대학원 정보경영학과

A Method for Quality Evaluation of Firewall

Ha-Yong Lee[1*], Won-Il Kweon[2] and Hae-Sool Yang[3]
[1]Seoul Univ. of Venture & Information
[2]STA Consulting Corp., [3]Graduate School of Venture, Hoseo Univ.

요 약 국제표준은 소프트웨어의 일반적인 특성과 공통성을 토대로 구축된 것이다. 따라서 특정한 지식정보보안 제품에 적용하기 위해서는 제품의 특성을 최대한 고려하고 관련 표준을 적용하여 평가 방법을 최적화하는 과정이 필수라 할 수 있다. 아울러, 소프트웨어 분야의 급격한 발전으로 인해 국제표준의 변화도 불가피하기 때문에 표준의 구성이나 내용이 지속적으로 변화되어 왔고 이러한 변화를 수용한 평가방법의 구축도 필요한 실정이다. 본 논문에서는 지식정보보안 제품 중 침입차단시스템(Firewall)의 품질수준을 평가하여 개선방향을 도출함으로써 품질향상을 지원할 수 있는 평가모델을 개발하였다. 이를 위해 침입차단시스템의 동향 및 기술적인 요소들을 조사 분석하고 침입차단시스템의 특성을 고려하여 일반 품질 요구사항과 고유한 품질 요구사항을 도출하고 품질평가 모델과 평가 방법을 제시하였다.

Abstract International standard is the documents that is constructed based on general and common characteristics of software. Thus, it is necessary to consider the characteristics of product and optimize the evaluation method by using related standard to adapt to some specific knowledge information security products. Also, because rapid development of software field was obliged to change the international standard, the content and construction of standard has changed, it is necessary to construct the evaluation method with this change. In this paper, we developed the evaluation model that can support the quality enhancement by evaluating the quality level and extracting the improvement method of firewall. For this, we surveyed and analyzed the trend and the technical elements of firewall and considering the general quality requirements and unique quality requirements, and proposed the quality evaluation model and method.

Key Words : Firewall, Knowledge Information Security, Quality Evaluation

1. 서론

지식정보보안 제품은 양적으로는 빠른 성장세를 보이고 있으나 그 동안 질적인 품질을 고려하는 노력이 미흡한 것이 사실이었다[1]. 따라서, 본 논문에서는 지식정보보안 제품의 질적인 면을 평가하여 품질수준을 파악하고 개선방향을 도출함으로써 품질향상을 지원할 수 있는 평가모델을 개발하기 위해 지식정보보안 분야의 대표 제품이라 할 수 있는 침입차단시스템(Firewall)을 대상으로 제품의 동향 및 기술적인 요소들을 조사 분석하고, 평가방법론 구축의 근간이 되는 국제표준의 동향을 분석하였다.

또한 침입차단시스템의 특성을 고려하여 일반 품질요구사항으로 커버되는 품질 요소와 침입차단시스템 고유의 품질 요구사항을 도출한 필요가 있는 요소를 분류하여 분석함으로써 보안성 및 보안성능이 지식정보보안제품의 품질평가에서 비중 있게 다루어질 수 있도록 하였다.

본 연구에서는 기존의 품질평가 모델에서 충분히 고려되지 않은 특정 제품별 품질평가 가능 모델을 침입차단시스템의 관점에서 제시하였으며 제시된 모델을 통해 지

*교신저자 : 이하용(lhyazby@suv.ac.kr)
접수일 10년 10월 06일 수정일 10년 12월 03일 게재확정일 10년 12월 17일

식정보보안 제품별 품질평가를 수행할 수 있도록 하였다. 또한, 지식정보보안 제품에 대해 기존 보안기능 중심의 평가에서는 다루지 못했던 비기능 요소를 포괄적으로 적용할 수 있는 품질평가 모델을 구축하였다.

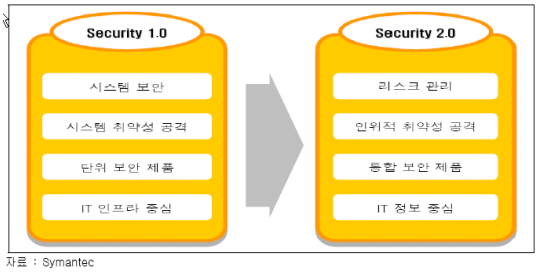
지금까지는 CC(Common Criteria) 인증[2, 3, 4]을 통해 지식정보보안 제품에 대한 보안기능 중심의 인증을 수행해 왔으나 제품의 포괄적인 품질을 다루고 있지 않다는 한계를 고려할 필요가 있으며 상기한 소프트웨어 제품 평가에 관한 국제표준의 적용에 따른 한계 및 ISO/IEC 25000 시리즈[5]로 표준이 변화해가고 있다는 점도 수용할 필요가 있다.

본 논문을 통해 침입차단시스템의 특성과 최신 표준화 동향을 반영하고 제품별 평가를 수행할 수 있는 평가모델을 구축함으로써 침입차단시스템의 전반적인 품질향상에 기여할 수 있을 것으로 사료된다.

2. 지식정보보안 분야의 동향

2.1 정보보안 패러다임의 변화[6]

최근의 보안위협은 게이트웨이 레벨에서 애플리케이션 레벨의 보안 이슈로 변화하고 있는 상황이다.



자료 : Symantec

[그림 1] 정보보호 패러다임의 변화

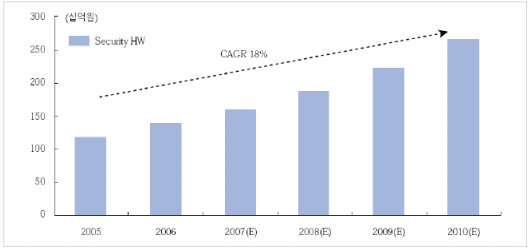
이에 따라 정보보안은 단순히 시스템에 보안 프로그램을 설치하는 것이 아닌 일련의 프로세스가 안전한 환경에서 이루어져야 한다는 인식이 확산되고 있으며, 이것이 최근 불고 있는 Security 2.0의 기본 개념이다.

Security 2.0 개념에 따라 침입차단시스템의 게이트웨이 레벨의 보안에 추가로 각종 애플리케이션과 엔드포인트를 제어하고 관리할 수 있는 전사적인통합관리 솔루션의 필요성이 대두되고 있다.

2.2 국내외 정보보안 시장 비교[7]

해외 정보보안 시장의 경우 보안 서비스 부문이 2005년부터 2009년까지 연평균 16.4%로 가장 높은 성장세를 보였다. 보안 하드웨어 및 소프트웨어 시장은 각각 16.8%와 12.9%의 성장세를 보였다.

이에 비해 국내 정보보안 시장은 하드웨어 부문의 성장세가 전체 보안 시장에서 가장 높은 것으로 나타나고 있다. 보안 HW 부문이 연평균 18%의 성장세로 보일 것으로 전망되며, SW 부문은 12%의 연평균 성장세를 보일 것으로 전망되고 있다.



(주) CAGR : Compound Annual Growth Rate(연평균성장률)

[그림 2] 국내 정보보안 하드웨어 시장 변화 및 전망

3. 침입차단시스템의 개요

3.1 침입차단시스템의 개념

침입차단시스템은 방화벽이라고도 하며 내부 네트워크를 외부의 공격으로부터 보호하기 위한 다양한 보안 장치와 기능들을 포괄적으로 포함한다.

방화벽 시스템은 시스템 자원을 원천적으로 보호하며 확실한 접근제어(Access Control)가 가능하고 보안 업무 집중으로 보안관리가 명확하고 용이해진다.

반면, 접속지연 시간이 증가하며 대역폭의 사용가능도가 축소되고 설치오류가 치명적일 수 있으며 내부사용자의 불법 행위에 대해 감시 효과가 거의 없다.

3.2 침입차단시스템의 특성

3.2.1 스크리닝 라우터(Screening Router)

스크리닝 라우터란 통신 프로토콜로서 발신지 주소와 목적지 주소, 통신 프로토콜의 제어 필드 그리고 통신 시 사용하는 포트 번호를 분석해서 내부 네트워크에서 외부 네트워크로 나가는 패킷 트래픽을 허가 및 거절하거나 혹은 외부 네트워크에서 내부 네트워크로 진입하는 패킷 트래픽의 진입허가 및 거절을 행하는 라우터를 말한다. 스크리닝 라우터는·필터링 속도가 빠르고, 비용이 적게 들며 네트워크 및 전송계층에서 동작하기 때문에 클라이

언트와 서버에 변화가 없어도 되고 사용자에 대해 투명성을 유지한다.

3.2.2 배스천 호스트(Bastion Host)

배스천 호스트는·외부 네트워크와 내부 네트워크의 접점에 위치하기 때문에 불법 침입자들의 최우선 공격 목표가 된다. 사실 어느 정도는 고의로 공격에 노출시키는 목적을 가진 호스트일 뿐만 아니라 방화벽의 주된 장치이므로 안전성이 완벽해야 한다. 배스천 호스트는 응용 서비스의 종류에 종속적이므로 스크리닝 라우터보다 안전성이 높으며 데이터에 대한 공격을 확실하게 방어할 수 있고 로그 정보의 생성 및 관리가 용이하다.

4. 침입차단시스템의 품질특성

이 장에서는 적용할 국제표준의 소프트웨어 품질평가 기준인 ISO/IEC 9126[8]과 ISO/IEC 25000 시리즈에 대해서 기술하고 이를 기반으로 침입차단시스템의 품질 요구사항을 분석하고 품질특성을 구축하였다.

4.1 침입차단시스템 평가에 적용할 관련 표준

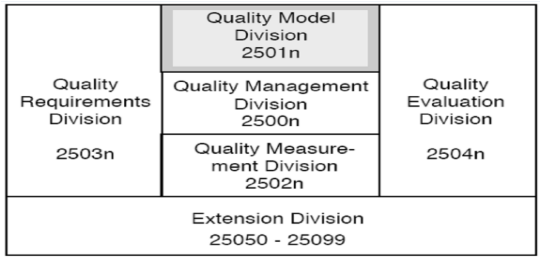
본 연구에서는 침입차단시스템의 품질 시험 및 평가 방법을 구축하기 위해 소프트웨어 제품평가에 관한 국제표준인 ISO/IEC 9126과, 일부 표준화 및 표준화가 진행중인 ISO/IEC 25000 시리즈를 기반으로 하였다.

4.1.1 ISO/IEC 9126

ISO/IEC에서는 소프트웨어 품질평가를 위한 모델과 이에 대한 평가절차를 표준으로 정하고 있으며, 특히 ISO/IEC 9126에서는 품질평가 모델이 규정되어 있다. ISO/IEC 9126-1에서는 내부품질(Internal Quality), 외부품질(External Quality), 사용품질(Quality in use) 측정을 위한 특성들을 규정한다. 내부품질은 소프트웨어의 원시코드 등이 얼마나 올바르게 작성이 되어 있는가를 뜻하며, 외부 품질은 소프트웨어가 데이터를 올바르게 처리하는 등의 성능을 의미한다. 사용 품질은 소프트웨어를 사용함에 있어 얼마나 편리한가 등을 나타낸다.

4.1.2 ISO/IEC 25000 시리즈

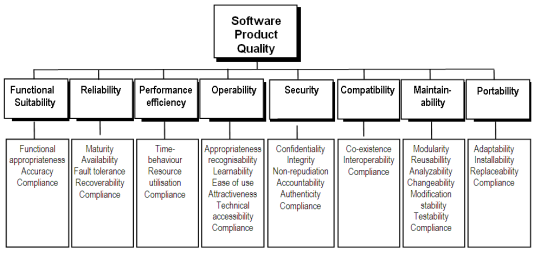
소프트웨어 제품 품질표준(ISO/IEC 9126)과 이를 평가하는 표준 (ISO/IEC 14598)은 통합되어야 한다는 주장에 따라 SQuaRE 프로젝트가 시작되었다. SQuaRE는 그림 9와 같이 용어정의, 참조모델과 설명, ‘shall’ 로 표시된 필수사항과 ‘should‘로 표시되는 추천사항, 각 장의 내용에 대한 설명으로 구성되어 있다.



[그림 3] SQuaRE의 Architecture

(1) Software Quality Model(CD 25010)

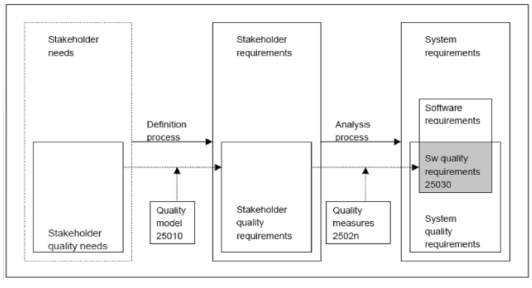
ISO/IEC25010에 정의된 소프트웨어 제품품질 모델은 그림 4와 같다. 품질특성은 8개로 정의되어 있으며 각 품질특성에 대한 부특성들이 정의되어 있다.



[그림 4] ISO/IEC 25010의 소프트웨어 제품 품질모델

(2) Software Quality Requirements(ISO/IEC 25030)

ISO/IEC 25030에서는 소프트웨어 품질 요구사항을 정의하고 있다. 소프트웨어 품질 요구사항은 그림 5와 같이 품질척도를 근간으로 도출된다.

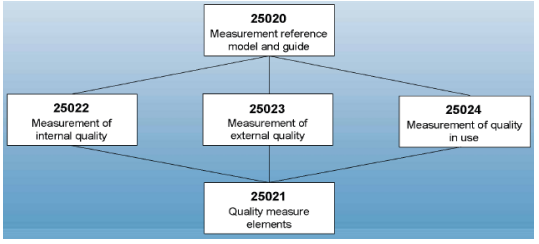


[그림 5] 소프트웨어 품질 요구사항

(3) Software Quality Measurement(ISO/IEC 2502n)

ISO/IEC 2502n에서는 소프트웨어 품질척도를 정의하

고 있다. ISO/IEC 25020은 척도 참조모델과 가이드, ISO/IEC 25021은 품질 척도 요소, ISO/IEC 25022는 내부품질 척도, ISO/IEC 25023은 외부품질 척도, ISO/IEC 25024는 사용품질 척도를 다루고 있다.



[그림 6] 소프트웨어 품질척도의 구성

(4) Evaluation reference Model and guide(ISO/IEC 25040)

ISO/IEC 25040은 평가 참조모델과 가이드를 포함하고 있으며 그 내용은 소프트웨어 품질의 명세와 평가에 관한 일반적인 요구사항, 소프트웨어 제품의 품질을 평가하고 이 프로세스의 응용을 위한 요구사항을 표현하기 위한 프로세스 기술(description)이다.

5. 침입차단시스템의 요구사항 분석

5.1 침입차단시스템의 일반적 요구사항

이 절에서는 일반적인 소프트웨어 제품과 유사한 지식정보보안 제품의 품질 요구사항에 대해 정리하였다. 본 연구에서 대상으로 하는 지식정보보안 제품은 침입차단시스템이며, 일반 품질 요구사항은 일부분을 제외하고 침입차단시스템이 다른 소프트웨어 분야와 유사하게 가지고 있는 요구사항들을 도출한 것이다.

5.1.1 기능성에 관한 요구사항

기능성에 관한 부특성으로는 적합성, 정확성, 상호운영성, 준수성이 있으며 요구사항을 정리하면 다음과 같다.

[표 1] 기능성에 관한 일반적 요구사항

부특성	요구사항
적합성	기능의 완전한 구현, 필수기능 구현, 기능의 적절성, 요구되는 수준의 침입차단기능
정확성	정확성 요구수준부합, 명세된 정밀도수준에 맞는 구현
상호운영성	명세된 대로 데이터 상호교환, 표준화된 자료 교환
준수성	기능 관련 표준이나 규약에 따라 동작

5.1.2 신뢰성에 관한 요구사항

신뢰성에 관한 부특성으로는 성숙성, 결함허용성, 회복성, 준수성이 있으며 요구사항을 정리하면 다음과 같다.

[표 2] 신뢰성에 관한 일반적 요구사항

부특성	요구사항
성숙성	결함개선 명시, 결함최소화
결함허용성	치명적인 결함의 최소화
회복성	결함의 완전환 복구, 결함으로 인한 사용불가능 시간 최소화, 복구시간 최소화, 복구가능
준수성	신뢰성 수준에 관한 표준이나 권고안, 규정에 따른 신뢰성 수준 준수

5.1.3 사용성에 관한 요구사항

사용성에 관한 부특성으로는 이해가능성, 학습가능성, 운영성, 선호도, 준수성이 있으며 요구사항을 정리하면 다음과 같다.

[표 3] 사용성에 관한 일반적 요구사항

부특성	요구사항
적합성	기능의 완전한 구현, 필수기능 구현, 기능의 적절성, 요구되는 수준의 침입차단기능
정확성	정확성 요구수준 부합, 명세된 정밀도수준에맞는 구현
상호운영성	명세된 대로 데이터 상호교환, 표준화된 자료 교환
준수성	기능 관련 표준이나 규약에 따라 동작

6.1.4 효율성에 관한 요구사항

효율성에 관한 부특성으로는 시간효율성, 자원효율성, 준수성이 있으며 요구사항을 정리하면 다음과 같다.

[표 4] 효율성에 관한 일반적 요구사항

부특성	요구사항
시간효율성	평균반응시간의 최소화, 평균처리량 수준 유지, 평균처리 시간 수준 유지
자원효율성	I/O 자원 사용의 최소화, 메모리 사용 최소화, 전송속도 수준 유지
준수성	효율성 관련 표준이나 관례에 따라 구현

6.1.5 유지보수성에 관한 요구사항

유지보수성에 관한 부특성으로는 분석성, 변경성, 안정성, 테스트용이성, 준수성이 있으며 요구사항을 정리하면 다음과 같다.

[표 5] 유지보수성에 관한 일반적 요구사항

부특성	요구사항
분석성	필요한 문제해결 정보의 적절한 제공, 모니터링 데이터의 기록/저장, 문제해결 정보에 따른 문제 해결 가능
변경성	환경설정 변경용이, 설정 변경에 따른 통제 용이
안정성	설정 변경에 따른 안정성 유지
테스트용이성	자체 시험기능 제공 등을 통한 테스트 지원
준수성	유지보수성 관련표준이나 관례에 따라 구현

6.1.6 이식성에 관한 요구사항

이식성에 관한 부특성으로는 적응성, 설치가능성, 대체성, 공존성, 준수성이 있으며 요구사항을 정리하면 다음과 같다.

[표 6] 이식성에 관한 일반적 요구사항

부특성	요구사항
적응성	필요한 문제해결 정보의 적절 제공, 모니터링 데이터의 기록/저장, 문제해결 정보에 따른 문제 해결 가능
설치가능성	환경설정 변경 용이, 설정 변경에 따른 통제 용이
대체성	설정 변경에 따른 안정성 유지
공존성	자체 시험기능 제공 등을 통한 테스트 지원
준수성	유지보수성 관련 표준이나 관례에 따라 구현

5.2 침입차단시스템의 고유 요구사항 분석

이 절에서는 침입차단시스템 고유의 품질 요구사항인 보안성과 보안성능에 관한 요구사항을 분석하였다.

5.2.1 보안성에 관한 요구사항[10]

5.2.1.1 보안감사

보안감사는 보안과 관련된 행동에 대한 책임을 추적하기 위해 지식정보보안 제품에서 발생하는 관련 사건들의 감사 레코드를 생성, 기록, 검토하고 감사된 사건에 대한 잠재적 보안 위반을 탐지하고 대응행동을 수행하는 능력을 의미하며, 보안감사에 관한 요구사항은 표 7과 같다.

[표 7] 보안감사에 관한 요구사항

요구사항	개 념
보안경보	잠재적인 보안 위반을 탐지한 경우 혼란을 최소화하는 대응행동의 목록을 취해야 한다.
감사데이터 생성	감사대상 사건들의 감사 레코드를 생성할 수 있어야 한다.(감사기능 시동/종료, 감사대상 사건 등)
규칙위반 지적	감사된 사건을 검사하는 경우에 규칙 집합을 적용할 수 있어야 하고, 이 규칙에 기반하여 잠재적 위반을 지적할 수 있어야 한다.
...	...

6.2.1.2 사용자 데이터 보호

사용자 데이터 보호란 지식정보보안 제품 장애 발생시 안전한 상태를 유지하고 보안 관련 데이터 및 실행코드의 무결성을 검증하기 위하여 자체 시험을 수행하며 사용자가 일정기간 컴퓨터를 사용하지 않는 상황이 발생했을 때 세션 관리 기능을 제공하는 능력을 의미한다.

[표 8] 사용자 데이터 보안 관한 요구사항

요구사항	개 념
정보흐름 통제	머도느 정보흐름 유발 오퍼레이션에 대하여 정보흐름통제를 강제해야 하며 모든 정보흐름을 유발하는 모든 오퍼레이션들의 정보흐름을 통제해야 한다.

5.2.1.3 식별 및 인증

식별 및 인증이란 해당 정보보호 제품의 관리자를 포함한 사용자의 신원을 식별 및 인증하고 인증 실패시 대응 행동을 제공하는 능력을 의미한다.

[표 9] 식별 및 인증에 관한 요구사항

요구사항	개 념
인증실패 처리	인증 사건의 목록에 관련된 정해진 횟수의 실패한 인증 시도가 발생한 경우 이를 탐지해야 한다.
사용자 보안속성 유지	각 사용자에 속한 디폴트값, 질의 , 변경, 삭제, 기타 연산 등의 보안속성 목록을 유지해야 한다.
비밀정보의 검증	비밀정보가 정의된 허용기준을 만족시킴을 검증하는 메커니즘을 제공해야 한다.
...	...

5.2.1.4 보안 관리

보안관리란 해당 지식정보보안 제품의 보안기능, 보안속성, 보안 관련 데이터, 보안 역할 등과 관련된 사항을 관리하는 능력을 의미한다.

[표 10] 보안 관리에 관한 요구사항

요구사항	개 념
보안기능 관리	기능목록의 기능에 대해 행동을 결정, 중지, 개시, 변경하는 능력을 인가된 관리자로 제한해야 한다.
보안속성 관리	보안속성목록의 보안속성을 디폴트값 변경, 질의, 변경, 삭제, 기타 연산하는 능력을 인가된 관리자로 제한하도록 접근통제, 정보흐름통제를 강제해야 한다.
데이터 관리 제한	식별 및 인증 데이터를 변경, 삭제하는 능력을 인가된 관리자로 제한해야 한다.
...	...

5.2.1.5 보안기능 보호

보안기능 보호란 보안기능에 대해 주기적 또는 관리자

의 요구에 따라 무결성을 검증하는 능력을 의미한다.

(1) 자체 시험

침입차단시스템은 보안기능의 정확한 운영을 입증하기 위하여 시동 시, 정규 운영 동안 주기적으로, 인가된 사용자 요구 시, 자체시험이 발생해야 하는 조건 시 자체 시험을 실행해야 한다.

5.2.1.6 접근통제

접근통제란 시스템이 정보흐름을 중재하기 위해 관련 보안 정책에 기반하여 패킷필터링 등을 통하여 외부망으로부터 내부망을 보호하는 능력을 의미한다.

[표 11] 접근통제에 관한 요구사항

요구사항	개 념
세션 잠금	인가된 관리자 비활동 기간 후 상호 작용하는 인가된 관리자 세션을 잠가야 한다.
세션 종료	사용자 비활동 기간 후에 상호작용하는 사용자 세션을 종료해야 한다.

6.2.2 보안성능에 관한 요구사항

(1) 최대 패킷 처리량(Throughput)

침입차단시스템이 패킷 손실 없이 처리할 수 있는 최대 트래픽 측정값인 최대 패킷 처리량은 규정된 수준 또는 제품 제공자가 명세한 수준을 유지해야 한다.

(2) 초당 연결수(Connectin Per Second)

침입차단시스템의 초당 연결수는 적정 수준이거나 제품 제공자가 명세한 수준을 유지하여야 한다.

(3) 초당 트랜잭션의 수(Transaction Per Second)

침입차단시스템의 초당 트랜잭션의 수는 적정 수준이거나 제품 제공자가 명세한 수준을 유지하여야 한다.

(4) 지연(Latency)

침입차단시스템이 처리할 수 있는 처리 용량의 규정된 수준에서 전송지연을 검증할 수 있어야 한다.

6. 침입차단시스템의 평가기준 및 방법론 구축

이 절에서는 침입차단시스템의 다양한 특징과 요구사항을 바탕으로 평가기준 및 방법론을 구축하였다.

6.1 품질평가 기준

본 논문에서는 품질평가 기준으로서 기능성, 신뢰성, 사용성, 효율성, 유지보수성, 이식성에 관한 기준을 구축하였다. 여기에서는 각 품질특성별로 일부를 제시하였다.

6.1.1 기능성 평가항목

기능성이란 지식정보보안 제품이 특정 조건에서 사용될 때, 명시된 요구와 내재된 요구를 만족하는 기능을 제공하는 제품의 능력을 의미한다. 기능성은 적합성, 정확성, 상호운영성, 준수성 등의 품질 부특성으로 세분화 된다. 기능성의 평가항목을 표 7에 나타내었다.

[표 7] 기능성의 평가항목

특성	부특성	평가 항목명	평가항목의 목적
기능성	적합성	기능구현 완전성	문서에 기술되어 있는 기능의 구현 여부
		기능 충분성	필요한 필수 기능의 충분한 구현 여부
		기능 적절성	평가된 각 기능이 침입차단 시스템을 구성하는 기능 요소로서 적절한지 여부를 평가
		침 입 차 단 적합성	보안기능에 관련해서 침입차단이 필요한 상황에 대해 차단이 어느정도 이루어지는지 평가
	정확성	기능 구현 정확성	각 기능이 명세대로 구현되어 요구수준에 부합하는지 여부를 평가
		정밀성	제품의 결과값이 사용자문서에 기술된 결과값의 정밀도와 동일하게 구현되어 있는지 여부
	…	…	…

6.1.2 보안성 평가항목

보안성이란 권한이 없는 사람 또는 시스템은 정보를 읽거나 변경하지 못하게 하고, 권한이 있는 사람 또는 시스템은 정보에 대한 접근이 거부되지 않도록 정보를 보호하는 지식정보보안 제품의 능력을 의미한다. 보안성은 보안감사성, 사용자 데이터 보호, 식별 및 인증, 보안관리성, 보안기능 보호, 접근통제성, 준수성 등의 평가항목을 가진다. 보안성의 평가항목을 표 8에 나타내었다.

[표 8] 보안성의 평가항목

특성	부특성	평가 항목명	평가항목의 목적
보안성	보 안 감 사 성	보안 경보	보안위반 탐지시 대응행동의 목록을 취하는가를 평가
		감사 데이터 생성	규정된 감사데이터를 생성하는지 평가

		...	...
	사용자 데이터 보호	정보흐름 통제	정보흐름과 관련된 기능의 정보흐름을 통제하는지 평가
		보안 속성에 따른 통제	보안속성에 따라 정보흐름을 통제하는지 평가
	식별 및 인증	인증 실패 처리	인증실패를 탐지하고 대응행동을 수행하는지를 평가
		사용자 보안 속성 유지	각 사용자에 대해 규정된 보안속성 목록을 유지하는지 평가
		...	...
	보안 관리성	보안기능 관리	인가된 관리자만 보안기능을 관리할 수 있도록 제한하는지 평가
		보안속성 관리	보안속성을 인가된 관리자만 다룰 수 있도록 제한하는지 평가
		...	...
	보안기능 보호	자체 시험	데이터 및 실행코드의 무결성을 검증하기 위해 자체 시험을 실행할 수 있는가를 평가
	접근 통제성	세션 잠금	관리자 비활동 기간 후에 세션을 잠가 활동을 무력화시키는지 평가
		세션 종료	사용자 비활동 기간후에 상호작용하는 사용자 세션을 종료하는지 평가
	준수성	보안성 표준 준수율	침입차단 시스템의 보안성 관련 표준, 기준 및 지침에 따라 시스템이 구현되어 있는지 평가

6.1.3 신뢰성 평가항목

신뢰성이란 명세된 조건에서 사용될 때, 성능 수준을 유지할 수 있는 지식정보보안 제품의 능력을 의미한다. 신뢰성은 성숙성, 결함허용성, 회복성, 준수성 등의 품질 부특성으로 세분화 된다. 신뢰성의 평가항목을 표 9에 나타내었다.

[표 9] 신뢰성의 평가항목

특성	부특성	평가 항목명	평가항목의 목적
신뢰성	성숙성	문제 해결률	이전 버전의 침입차단 시스템에 존재하던 문제에 대하여 명시적으로 해결이 확인되는 정도를 평가
		결함 회피율	일정한 운용 시간 내에 결함이 발생하지 않는 정도를 평가
		결함발생 평균시간	침입차단 시스템의 결함발생 평균시간을 평가
	결함 허용성	다운 회피율	발생되는 결함 중 시스템 다운을 가져오는 결함이 발생하지 않는 정도
		장애 회피율	발생되는 결함 중 장애를 발생시키는 정도의 심각한 결함이 발생하지 않는 정도
	...	...	...

6.1.4 사용성 평가항목

사용성이란 명시된 조건에서 사용할 경우 사용자가 이해하고, 학습하고, 사용하며 선호할 수 있는 지식정보보안 제품의 능력을 의미한다. 사용성에는 이해가능성, 학습 가능성, 운영성, 선호도, 준수성 등의 품질 부특성으로 세분화 된다. 사용성의 평가항목을 표 10에 나타내었다.

[표 10] 사용성의 평가항목

특성	부특성	평가 항목명	평가항목의 목적
사용성	이해 가능성	기능 이해도	제품 설명서와 사용자 문서를 읽고 제품이 제공하는 기능을 이해할 수 있는 정도를 평가
		인터페이스 이해도	제품의 메뉴 및 기타 인터페이스를 보고 기능을 이해 할 수 있는 정도
		도움말 이해도	제품에서 제공하는 도움말을 쉽게 이해할 수 있는 정도
		...	...
	학습 가능성	기능 학습 용이성	사용자가 제품을 사용하기 위한 기능을 쉽게 학습할 수 있는 정도
		도움말 접근용이성	사용자가 도움말을 쉽게 참조할 수 있는 정도
	...	...	...

6.1.5 효율성 평가항목

효율성이란 명시된 조건에서 사용되는 자원의 양에 따라 요구된 성능을 제공하는 지식정보보안 제품의 능력을 의미한다. 효율성에는 시간 효율성, 자원 효율성, 성능, 준수성 등의 품질 부특성으로 세분화된다. 효율성의 평가항목을 표 11에 나타내었다.

[표 11] 효율성의 평가항목

특성	부특성	평가 항목명	평가항목의 목적
효율성	시간 효율성	평균반응 시간의 적절성	제품 사용 시의 사용자의 입력에 대한 평균반응 시간을 측정
		평균 처리율	제품이 주어진 시간내에 성공적으로 작업을 수행할수 있는 평균처리량을 측정
		평균처리 시간의 적절성	제품 사용 중 특정한 업무를 성공적으로 수행하는 평균 처리 시간
	자원 효율성	입출력 자원 사용률	침입차단시스템의 I/O자원의 사용정도
		메모리 사용률	침입차단시스템의 메모리사용 정도
		데이터 전송률	침입차단시스템의 데이터전송 속도

		CPU 사용률	침입차단시스템의 CPU 사용 정도
	보안성능	Throughput	최대 패킷 처리량(throughput)을 측정. 장비가 패킷 손실 없이 처리할 수 있는 최대 트래픽 측정(
		CPS(Connection Per Second)	초당 연결수가 적정 수준인가를 측정
		…	…

6.1.6 유지보수성 평가항목

유지보수성이란 지식정보보안 제품이 변경되는 능력을 의미한다. 변경에는 환경과 요구사항 및 기능적 명세에 따른 지식정보보안 제품의 수정, 개선, 또는 개작 등이 포함된다. 유지보수성은 분석성, 변경성, 안정성, 테스트 용이성, 준수성 등의 품질 부특성으로 세분화 된다. 유지보수성의 평가항목을 표 12에 나타내었다.

[표 12] 유지보수성의 평가항목

특성	부특성	평가 항목명	평가항목의 목적
유지보수성	분석성	진단기능 지원률	제품 사용시 발생하는 결함의 증상 및 상태를 해결할 수 있는 진단 기능 제공 정도
		감사추적 가능성	상태를 모니터링하기 위한 필요한 데이터를 기록 저장하는 기능 제공 정도
		문제해결 구현율	문제해결 정보에따라 발생한 문제를 해결하는 정도
	변경성	변경 가능성	제품에서 환경 설정을 변경하기 용이하게 구현되어 있는지의 정도
		변경 통제 가능성	제품의 변경 또는 환경 설정 변경에 대한 통제가 용이한 정도
	…	…	…

6.1.7 이식성 평가항목

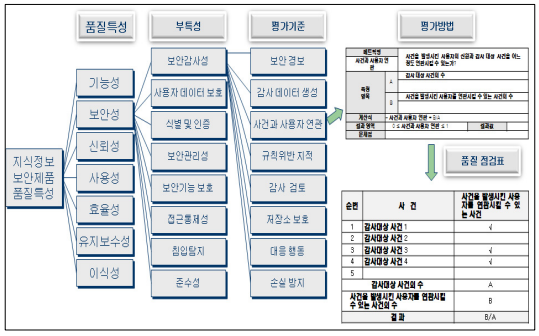
이식성이란 한 환경에서 다른 환경으로 전이될 수 있는 지식정보보안 제품의 능력을 의미한다. 이식성에는 적응성, 설치가능성, 대체성, 공존성, 준수성 등의 품질 부특성으로 세분화된다. 이식성의 평가항목을 표 13에 나타내었다.

[표 13] 이식성의 평가항목

특성	부특성	평가 항목명	평가항목의 목적
이식성	적응성	데이터 구조 적응률	현재 환경에서의 데이터 구조에 제품이 적응하는 정도
		적용 환경	서로 다른 환경이나 하드웨어, 시스템 소프트웨어 환경에서 제품이 사용될 수 있
		적응률	도록 제품이 구현되어 있는 정도
		…	…
	설치 가능성	설치 가능률	제품 설치 정보에 따라 설치할 수 있도록 제품이 구현되어 있는 정도
		제거 가능률	제품을 제거 정보와 제거 제품을 이용하여 제거할 수 있도록 구현되어 있는 정도
	…	…	…

6.2 품질평가 방법

품질평가 방법은 그림 7과 같이 품질평가 기준을 측정하는 방법을 기술하는 품질 측정 지표로 구성된다. 그리고, 품질 측정 지표를 이용한 측정 자체는 품질 점검표를 통해 이루어진다.



[그림 7] 품질평가 방법의 구조

6.2.1 평가방법 개발 내역

평가방법은 품질시험에 관한 전반적인 사항을 정리한 것으로 측정지표명, 개념, 측정항목, 계산식, 결과 영역, 결과값, 문제점 기술 등을 정리한 표이다.

본 연구를 통해 표 13과 같이 침입차단시스템에 관해 95개의 평가방법을 구축하였다.

[표 13] 침입차단시스템에 관한 평가방법 개발 내역

품질특성	부특성	시험모듈 개발 내역	계
기능성	적합성	<기능구현완전성> 외 3개	15
	정확성	<기능구현정확성> 외 1개	
	상호운영성	<데이터교환성>	
	준수성	<기능성표준준수율>	
보안성	보안감사성	<보안경보> 외 6개	24
	사용자데이터보호	<정보흐름통제> 외 1개	
	식별 및 인증	<인증실패처리> 외 4개	
	보안관리성	<보안기능관리> 외 6개	
	보안기능보호	<자체시험>	
	접근통제성	<세션잠그> 외 1개	
	준수성	<보안성표준준수율>	
…	…	…	…
이	적응성	<데이터구조적응률> 외 2개	9

식성	설치가능성	<설치가능률> 외 1개	
	대체성	<데이터지속가능률> 외 1개	
	공존성	<공존가능률>	
	준수성	<이식표준준수율>	
계	34		95

6.2.2 평가방법의 도표화

이 절에서는 침입차단시스템의 품질평가 기준에서 정의된 평가 항목에 대해 평가개념을 기술하고 구체적인 측정항목 구성, 측정항목으로부터 메트릭의 결과를 도출하기 위한 계산식을 정의하고 계산 결과의 영역에 대해 기술한 평가방법을 표 14에 도표화하여 정리하였다.

[표 14] 평가방법의 도표화 예

메트릭명		인가되지 않은 삭제로부터 감사 레코드를 보호하는가?	
저장소 보호			
측정항목	A	인가되지 않은 삭제 시도의 수	
	B	감사 레코드가 삭제되지 않은 경우의 수	
계산식	- 저장소 보호 = A		
결과영역	0 ≤ 저장소 보호 ≤ 1	결과값	
문제점			

6.2.3 시험결과서

품질검사표에 대한 측정이 수행되면 각 메트릭별 측정결과가 산출될 수 있다. 이 결과들을 품질특성, 부특성에 대한 메트릭별로 표 15와 같은 시험결과서로 정리된다. 시험결과서는 각 메트릭별 결과값을 파악할 수 있으며 상대적으로 취약한 품질 항목을 확인하고 “메트릭 - 부특성 - 품질특성”의 단계에 따라 집계하여 종합적인 결과값을 도출할 수 있다.

[표 15] 시험결과서의 예

침입차단시스템의 제품설명서 및 사용자 문서			
품질특성	부특성	메트릭	측정값
기능성	적합성	기능구현 완전성	
		기능 충분성	
		기능 적절성	
		침입차단 적합성	
	정확성	기능구현 정확성	
		정밀성	
	…	…	…
…	…	…	…
이식성	적응성	데이터구조 적응률	
		적용환경 적응률	
		이식편리성	
	…	…	…
	공존성	공존가능률	
	준수성	이식성표준 준수율	

7. 품질 측정과 평가 사례

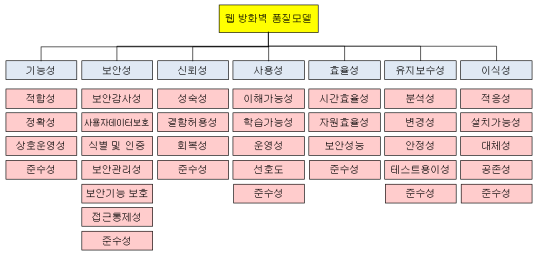
본 평가 사례에서는 침입차단시스템을 대상으로 평가를 수행하여 품질을 측정하고 평가한 사례를 통해 평가방법에 대해 소개하고자 한다.

7.1 개요

본 평가사례는 PC의 정보유출을 방지하는 온라인 PC 방화벽 프로그램에 대해 수행한 것이다. 대상 제품은 개인 방화벽 기능, 실시간 프로세스 모니터링 기능, 로그 기능, 환경 설정 기능, 도움말 등다음과 같은 기능을 가지고 있다.

7.2 평가모형

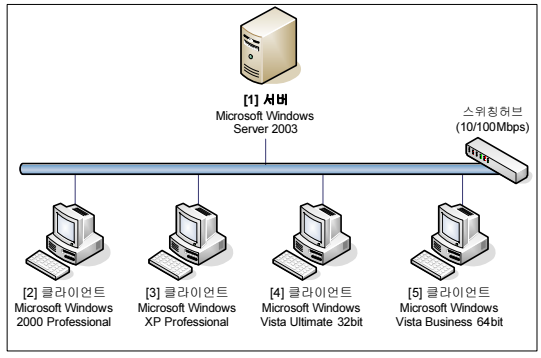
본 시험결과는 ISO/IEC 9126(소프트웨어 품질특성과 측정지표에 관한 국제표준)과 ISO/IEC 25000 시리즈의 표준화 동향을 고려하여 본 연구에서 개발된 그림 8과 같은 품질 평가 모형을 기준으로 시험항목을 설정하였다.



[그림 8] 평가모형

7.3 시험환경

침입차단시스템의 시험을 위해 구성한 시험환경은 그림 9와 같다.



[그림 9] 시험환경

7.3.1 서버

[1]번 서버에 설치한 프로그램은 웹서버 IIS v6.0과 서버 모듈이다.

7.3.2 클라이언트

[2]~[5]번 클라이언트에 설치한 프로그램은 Microsoft Internet Explorer v6.0, v7.0, v8.0과 Mozilla FireFox v2.0, v3.0이며 일반 응용 프로그램:으로 MS-Office 2003, 한글 2005, Window Media Player v9.0 등이다.

7.3.3 네트워크

네트워크로는 10/100 Mbps 스위칭 허브를 사용한다.

7.3.4 성능측정도구

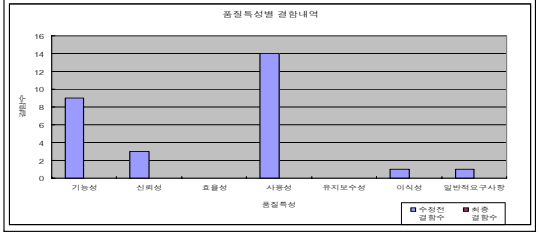
성능측정 도구는 Performance Logs and Alerts로서 시험 대상 제품 자원 사용률을 측정하며 [3]번 클라이언트에 설치하였다.

7.4 시험결과

7.4.1 품질특성별 결함 내역

시험과정은 1차시험을 거친 후 결함 내역을 산출하고 결함에 대한 수정/보완을 실시한 후 최종 시험을 수행하였다.

품질특성	수정전 결함수	최종 결함수
기능성	9	0
보안성	0	0
신뢰성	3	0
효율성	0	0
사용성	14	0
유지보수성	0	0
이식성	1	0
일반적 요구사항	1	0
계	28	0

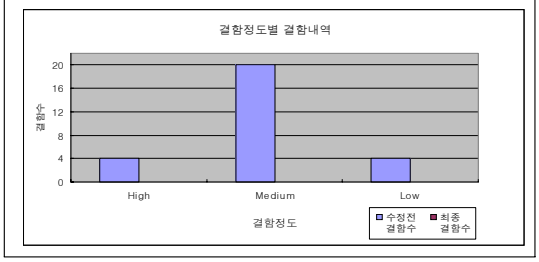


[그림 10] 품질특성별 결함 내역

7.4.2 결함 정도별 결함 내역

1차 시험을 통해 발생된 결함에 대해 결함 정도별로 결함을 분류하였다. 결함정도에서 High는 기능의 비정상 동작이나 종료 등의 치명적인 결함을 의미하며 Medium은 운영에는 문제가 없으나 정확하게 동작하지 않거나 사용자 혼란을 야기하는 정도의 결함이 발생하는 경우를 의미한다. Low는 문제 없이 정확히 동작하나 권고사항 수준의 경미한 결함이 발생하는 경우이다.

결함정도	수정전결함수	최종결함수
High	4	0
Medium	20	0
Low	4	0
계	28	0



[그림 11] 결함 정도별 결함 내역

7.5 품질특성별 시험결과

품질특성별 시험결과를 종합해 보면 수정 전 결함내역은 표 17과 같다.

[표 17] 수정 전 결함내역

번호	시험환경	결함	정도	품질특성	설명
1	시험환경 모든OS	바이러스/스파이웨어 치료 기능 오류	H	기능성	[온라인 스캐너>검사하기] 탐지된 일부 바이러스(예:NetBus)가 치료되지 않음
2	Microsoft Windows Vista Business 64bit	공유 폴더 표시기능 오류	M	기능성	[공유폴더] '공유 폴더' 정보를 갱신할 경우, '공유폴더'의 폴더명만 표시되어야 하지만, 자신의 PC 정보(예:PC160)도 함께 표시됨
…	…	…	…	…	…
27	시험환경 모든OS	프로그램 설치 오류	H	이식성	[설치] InternetExplorerv6.0,v7.0,v8.0 및 Mozilla FireFox v2.0에서 제품 설치 후 재실행을 요구하는 메시지가 계속 나타나며 제품이 실행되지 않음

7.6 성능시험 결과

성능시험은 시관효율성과 자원효율성을 측정하였으

며, 성능시험에 관한 측정항목은 표 18과 같다.

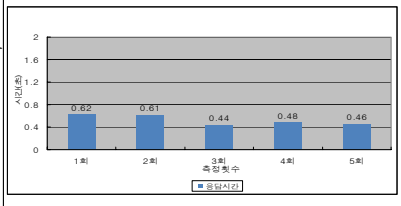
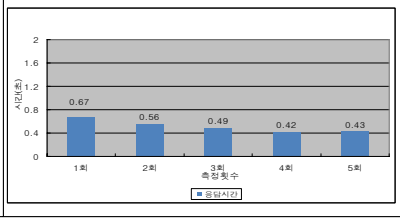
[표 18] 성능시험 측정항목

항목	단위	내용
CPU 사용률	%	%Processor Time: 비유휴 스레드를 실행하는데 소비하는 시간의 백분율
메모리 사용량	MB	Free Mbytes : 사용 가능한 실제 메모리의 양
응답시간	초	시스템에 조회나 요구 등의 명령을 입력한 직후부터 해당 명령의 처리가 완료된 시점까지 소요된 시간
Throughput	MByte/Sec	단위시간(Sec)당 작업 처리량

7.6.1 시간 효율성

(1) 응답시간

악성 프로세스 탐지 및 삭제할 경우와 응용 소프트웨어에 대해서 접속 허가를 실행할 경우, 응답시간이 각각 평균 0.8초, 0.5초가 소요되었다.

시나리오	측정결과
SC_2 (응용 소프트웨어에 대해서 접속 허가를 실행함)	[3]클라이언트(Microsoft Internet Explorer v8.0) – 응답시간  [3]클라이언트(Firefox v2.0) – 응답시간 

[그림 12] 시간효율성 측정결과(예)

7.6.2 자원 효율성

(1) CPU 사용률

Internet Explorer v8.0와 Mozilla FireFox v2.0에서 제품 구동 후 악성 프로세스를 탐지 및 삭제할 경우, [3]클라이언트의 CPU 사용률은 각각 18% 미만으로 올라갔으나 실행 완료 후 안정적으로 유지되었다.

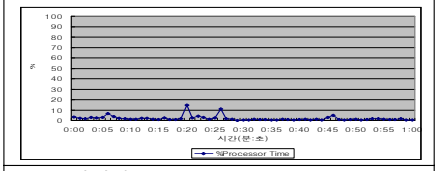
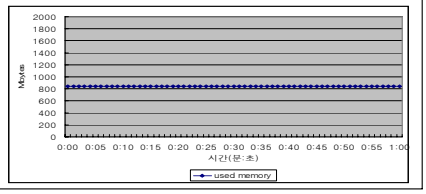
Internet Explorer v8.0와 Mozilla FireFox v2.0에서 제품구동후 응용소프트웨어에 대해서 접속허가를 실행할 경우, [3]클라이언트의 CPU사용률은 각각 22% 미만으로 올라갔으나 실행완료 후 안정적으로 유지되었다.

(2) 메모리 사용량

Internet Explorer v8.0와 Mozilla FireFox v2.0에서 제품 구동 후 악성 프로세스를 탐지 및 삭제할 경우, [3]클라이언트의 메모리 사용량은 각각 평균 843.7MB, 778.1MB로 나타났다.

Internet Explorer v8.0와 Mozilla FireFox v2.0에서 제품 구동 후 응용 소프트웨어에 대해서 접속 허가를 실행할 경우, [3]클라이언트의 메모리 사용량은 각각 평균 864.1MB, 847.1MB로 나타났다.

자원효율성에 관한 측정결과의 예를 그림 13에 나타내었다. CPU 사용률, 메모리 사용량 등의 경우, 사용률이나 사용량의 과다로 다른 작업에 지속적 영향을 주지 않는다면 지장 없는 것으로 판단하였다. CPU 사용률이나 메모리사용량은 다른 작업에 영향을 줄만큼 과다한 수준으로 오르지 않았으며 그 수준도 잠시 유지되고 곧 안정상태로 되돌아가므로 문제가 없다 판단된다.

시나리오	측정결과
SC_1 (악성 프로세스를 탐지 및 삭제함)	[3]클라이언트(Microsoft Internet Explorer v8.0)-CPU사용률  [3]클라이언트(Microsoft Internet Explorer v8.0) – 메모리사용량 

[그림 13] 자원효율성 측정결과(예)

7.7 종합평가 결과

평가 항목에 따른 품질특성별 세부 평가 결과는 표 19와 같다.

[표 19] 품질특성별 세부 평가결과

품질특성	품질부특성	평가결과	비고
기능성	적합성	1.00	
	정확성	1.00	

	상호운영성	1.00	
	보안성	1.00	
	준수성	NA	관련 표준 없음
신뢰성	성숙성	1.00	
	결함허용성	1.00	
	회복성	1.00	
	준수성	NA	관련 표준 없음
효율성	시간효율성	1.00	
	자원효율성	1.00	
	준수성	NA	관련 표준 없음
사용성	이해가능성	1.00	
	학습성	1.00	
	운영성	1.00	
	선호도	1.00	
	준수성	NA	관련 표준 없음
유지보수성	분석성	1.00	
	변경성	1.00	
	안정성	1.00	
	시험가능성	NA	해당 사항 없음
	준수성	NA	관련 표준 없음
이식성	적응성	1.00	
	설치가능성	1.00	
	대체성	NA	해당 사항 없음
	공존성	1.00	
	준수성	NA	관련 표준 없음
일반적 요구사항	식별 및 표시	1.00	
	안전성	1.00	

본 제품은 개인 PC의 정보유출을 방지하는 온라인 PC 방화벽 프로그램으로, 제공된 기능이 정확히 동작하는지, 프로그램 구성 요소들이 유기적으로 잘 동작하는지, 인터페이스는 편리한지, 사용자를 위한 사용자 설명서 내용은 충실한지, 유지보수는 용이한지 등을 중점적으로 평가하였다.

시험 과정에서 결함이 발생하였으나, 수정보완 및 회귀시험 과정을 거친 후 제품에서 제공하는 개인 방화벽 기능, 실시간 프로세스 모니터링 기능, 로그 기능, 환경설정 기능, 도움말 등이 정상적으로 동작하였으며, 일정 운영 시간 동안 프로그램에 치명적인 영향을 미치는 중대 결함은 발견되지 않았다.

Microsoft Internet Explorer v8.0와 Mozilla FireFox v2.0에서 제품 구동 후 악성 프로세스를 탐지 및 삭제할 경우, [3]클라이언트의 CPU 사용률은 각각 18% 미만으로 올라갔으나 실행 완료 후 안정적으로 유지되었으며, 메모리 사용량은 각각 평균 843.7MB, 778.1MB로 일정하게 나타났다. 응용 소프트웨어에 대해서 접속 허가를 실행할 경우, [3]클라이언트의 CPU 사용률은 각각 22% 미만으로 올라갔으나 실행 완료 후 안정적으로 유지되었으며, 메모리 사용량은 각각 평균 864.1MB, 847.1MB로 일정하게 나타났다. 또한, 악성 프로세스 탐지 및 삭제할 경우와 응용 소프트웨어에 대해서 접속 허가를 실행할 경우, 응답시간이 각각 평균 0.8초, 0.5초가 소요되었다.

직관적인 인터페이스를 사용하여 기능 및 구조를 쉽게 파악할 수 있었고, 도움말에 제품 사용 방법을 상세히 제공하여 기능 학습이 용이하였고, 제품 실행 중 자주 발생할 수 있는 문제에 대한 해결정보(예:FAQ)가 홈페이지에 제공되어 제품 사용이 편리하였다.

7.8 기존 평가 방법과의 비교분석

이 절에서는 지금까지 연구하여 제시된 다양한 평가방법들과 본 연구를 통해 제시한 평가방법을 비교분석하여 장단점을 파악할 수 있도록 하였다.

평가 툴을 이용하여 소스코드의 복잡도를 평가하는 방법은 코드 자체를 입력으로 하여 복잡도 척도를 평가하는 방법으로 자동화하여 효율적인 평가가 가능하지만 적용 대상이 실행가능한 소프트웨어에 한정되며 특정 프로그래밍 언어를 대상으로 한다는 한계가 있다.

체크리스트 이용 품질평가 방법은 사전에 효과적인 체크리스트를 보유하고 있다면 소프트웨어 개발 전 과정에 걸쳐 광범위하게 적용할 수 있는 방법이다. 구현된 실행가능한 소프트웨어뿐만 아니라 개발과정에서의 중간산출물에도 적용할 수 있어 평가범위가 넓으나 중간산출물에 대한 평가결과가 반드시 소프트웨어 제품의 평가를 정확히 대변하지 못한다는 점에서 한계가 있다.

품질평가 모듈은 침입차단시스템의 품질 요구사항과 특성을 분석하여 그 결과를 바탕으로 구축되었으므로 범용적인 평가방법이 아닌 특성화된 평가방법으로서 상대적으로 평가결과의 타당성을 제고할 수 있는 방법이다. 다만, 특정 소프트웨어 제품 또는 한정된 특성을 갖는 제품군의 품질평가에만 적용될 수 있는 한계가 있다.

[표 20] 품질평가 방법의 장단점 비교

평가방법	장점	단점
소스 코드 복잡도 평가 도구	소스코드의 복잡도를 평가하는 방법은 코드 자체를 입력으로 하여 복잡도를 평가하며 자동화를 통해 효율적인 평가가 가능하고 S/W의 유지보수 품질을 높일 수 있는 장점이 있다	적용 대상이 실행가능한 소프트웨어에 한정되며 특정 프로그래밍 언어를 대상으로 한다는 점에서 한계가 있다.
체크리스트를 활용한 품질점검	소프트웨어 개발 전 과정에 걸쳐 광범위하게 적용할 수 있고 구현된 소프트웨어뿐만 아니라 개발과정에서의 중간산출물에도 적용할 수 있어 평가범위가 넓은 장점이 있다.	중간산출물에 대한 평가결과가 반드시 소프트웨어 제품의 평가를 정확히 대변하지 못한다는 점에서 한계가 있다.
품질평가 모듈을 적	품질평가모듈은 침입차단시스템의 품질 요구사항과 특성 분석 결과를 바탕으로 구축되므로 범용적	특정 소프트웨어 제품 또는 한정된 특성을 갖는 제품군의

용한 품질 평가	인 평가방법이 아닌 특성화된 평가방법으로 상대적으로 평가결과의 타당성을 제고할 수 있는 방법이다.	품질평가에만 적용될 수 있는 한계가 있음

8. 결론

소프트웨어의 품질평가를 위한 기준이 되는 국제표준은 소프트웨어의 일반적인 특성과 공통성을 토대로 구축된 것이기 때문에 특정한 제품에 적용하기 위해서는 제품의 특성을 최대한 고려하여 표준을 적용하고 최적화하는 과정이 필수라 할 수 있다.

본 연구에서는 침입차단시스템의 특성을 고려하고 각 제품별 일반 품질요구사항으로 커버되는 품질 요소와 지식정보보안 제품의 고유한 품질 요구사항을 도출한 필요가 있는 요소를 분류하여 분석함으로써 보안성 및 보안성능이 지식정보보안제품의 품질평가에서 비중 있게 다루어질 필요가 있다는 결론을 도출하였다.

따라서 본 연구에서는 기존의 품질평가 모델에서 충분히 고려되지 않아 한계로 지적되었던 제품별 품질평가 가능 모델을 제시하였으며 제시된 모델을 통해 침입차단시스템의 품질평가를 수행할 수 있도록 하였다. 또한, 기존 보안기능 중심의 평가에서는 다루지 못했던 비기능 요소를 포괄적으로 적용할 수 있는 품질평가 모델을 구축하였다.

이번 연구는 지금까지 소프트웨어 제품군을 대상으로 한 품질평가 방법에 대한 연구는 활발히 수행되었으나 제품별 평가모델에 대한 연구사례가 부족한 관계로 연구결과의 타당성을 제고할 수 있는 관련 연구의 참조 사례를 확보하기 어려웠으며 이로 인해 평가 항목에 대한 타당성 검증이 미흡했다는 점이 다소 아쉬운 부분이라 할 수 있다.

향후 연구에서는 침입차단시스템을 위시한 지식정보보안 제품에 대한 품질평가 방법의 구축 및 지속적인 시험평가를 통해 사례를 축적함으로써 평가방법론의 타당성을 제고할 필요가 있다.

참고문헌

[1] 권원일, “지식정보보안 제품별 품질평가 방법론 연구”, 한국인터넷진흥원 위탁연구과제 최종보고서, 2009. 11.

[2] ISO/IEC 15408-1:2009 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model.

[3] ISO/IEC 15408-2:2008 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 2: Security functional components.

[4] ISO/IEC 15408-3:2008 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 3: Security assurance components.

[5] ISO/IEC 25000:2005 Software Engineering -- Software product Quality Requirements and Evaluation (SQuaRE) -- Guide to SQuaRE.

[6] 홍만표 역, Panko, R. Raymond, "정보보호개론 (Corporate Computer and Nework Security)", 한티미디어, 2006.

[7] IDC, "세계 정보보호산업 시장 전망 보고“, 2008.

[8] ISO/IEC 9126, “Information Technology - Software Quality Characteris- tics and metrics - Part 1, 2, 3".

[9] ISO/IEC 14598, "Information Technology - Software product evaluation - Part 1,2,3,4,5,6".

[10] 한국정보보호진흥원, “침입차단시스템 보호프로파일 V2.0”, 2008. 4.

[11] Azuma, M., "Software Quality Evaluation System : Quality Models, Metrics and Processes - International Standards and Japanese Practice", Information and Software Technology, 1996.

[12] Moller, K.H. and Paulish, D.J., "Software Metrics", Chapmen & Hall(IEEE Press), 1993.

[13] ISO/IEC 12119, "Information Technology - Software Package - Quality requirement and testing".

[14] 정지환, 김상영, 황션명, “네트워크 보안성능 평가 방법에 관한 연구”, 2001.

[15] KISA 연구보고서, “통합시스템 보안성 평가체계 및 방법 연구”, 2006.

[16] KISA 연구보고서, “정보보호제품 성능시험 및 보안 취약성 분석 연구”, 2002.

이 하 용(Ha-Yong Lee) **[정회원]**

- 1993년 2월 : 원대학교 전자계산학과 졸업(이학사)
- 1995년 2월 : 강원대학교 대학원 전자계산학과 소프트웨어공학 전공(이학석사)
- 2005년 2월 : 호서대학교 벤처전문대학원 컴퓨터응용기술학과졸업(공학박사)
- 1996년 3월 ~ 2005년 2월 : 경희대, 경원대, 선문대, 호서대 컴퓨터공학부 강사
- 1995년 ~ 2002년 : 한국S/W품질연구소 선임연구원
- 2005년 2월 ~ 현재 : 서울벤처정보대학원대학교 교수

<관심분야>
소프트웨어공학(특히, S/W 품질보증과 품질평가, 품질감리, 객체지향 프로그래밍, 객체지향 분석과 설계, 컴포넌트기반 S/W 개발방법론, 품질평가)

권 원 일(Won-Il Kweon) **[정회원]**

- 1997년 2월 : Auckland대학교 Information Systems (경영학사)
- 2000년 2월 : KAIST ICT IT경영전략 전공(경영학석사)
- 2000년 ~ 2004년 : ETRI(한국전자통신연구원), TTA(한국정보통신기술협회) SW 품질 시험 및 인증 연구원
- 2006년 ~ 현재 : (주)STA컨설팅 대표
- 2005년 ~ 현재 : 한국SW테스팅자격위원회(KSTQB) 대표
- 2007년 ~ 현재 : ISO/IEC 29119 SW테스팅 국제표준화 위원 (지식경제부 기술표준원 위임)
- 2008년 2월 ~ 현재 : 국립강원대학교 초빙교수

<관심분야>
소프트웨어 테스팅, 품질평가, 요구공학

양 해 술(Hae-Sool Yang) **[정회원]**

- 1975년 2월 : 홍익대학교 전기공학과 졸업(학사)
- 1978년 2월 : 성균관대학교 정보처리학과 졸업(석사)
- 1991년 2월 : 日本 오사카대학 정보공학과 S/W공학 전공(공학박사)
- 1975년 ~ 1979년 : 육군중앙경리단 전자계산실 시스템분석장교
- 1980년 3월 ~ 1995년 2월 : 강원대학교 전자계산학과 교수
- 1986년 ~ 1987년 : 日本 오사카대학교 객원연구원
- 1995년 ~ 2002년 : 한국소프트웨어품질연구소 소장
- 1999년 3월 ~ 현재 : 호서대학교 벤처전문대학원 교수

<관심분야>
S/W공학(특히, S/W 품질보증과 품질평가, 품질감리 및 컨설팅, OOA/OOD/OOP, SI), S/W 프로젝트관리, 품질경영