사례분석을 통한 ESM S/W의 평가항목

Evaluation Items of ESM S/W by Case Analysis

강득수, 양해술
호서대학교 벤처전문대학원

Deuk-Soo Kang(kdskmit@naver.com), Hae-Sool Yang(hsyang@hoseo.edu)

요약

ESM이란 방화벽, 침입탐지시스템(IDS), 가상시설망(VPN) 등 다양한 종류의 보안 솔루션을 하나로 모은 통합보안관리시스템으로 본 연구에서의 ESM 소프트웨어의 품질평가 모델을 개발하는 것은 ESM 소프트웨어를 효과적으로 보호하기 위한 기초가 된다고 할 수 있다鵡 본 논문에서는 ESM 소프트웨어 분야 기반기술을 조사하고 ESM 소프트웨어 기술, 시장, 표준 및 시험・인증 동향을 조사, 분석하여 ESM 소프트웨어의 평가 모델을 개발하고자 한다. 즉, ESM 소프트웨어의 요구사항을 반영하여 시험 모듈을 개발하여 시험방법과 더불어 시험사례를 제안하였다.

■ 중심어 : | 통합보안관리시스템 | 평가 모델 | 평가 방법 |

Abstract

ESM can do and wishes to investigate ESM software field base technology and investigate ESM software technology, market, standard and evaluation·certification trend and develop evaluation model of ESM software that it becomes foundation to protect ESM software effectively that develop quality evaluation model of ESM software in this research by integration security administration system that gather fire wall, IDS, VPN etc. various kind of security solution by one. That is, because reflecting requirement of ESM software, develop evaluation module and proposed evaluation example along with method of exam.

■ keyword : | ESM | Evaluation Module | Evaluation Example |

1. 서 론

IT(Information Technology)를 기반으로 하지 않은 비즈니스는 없다고 해도 과언이 아닐 정도로, 대부분의 비즈니스업무는 물론 일상생활까지 모두 컴퓨터 시스템의 도움을 받아 처리되고 있으며 정보 공유성을 극대화하기 위해 인터넷을 매개로 하는 개방형 네트워크 컴퓨팅 환경이 일반화 된 현재는 열린 환경 속에서 개인적인 정보 자산을 지키기는 일이 무엇보다 중요하다.

이런 사실과 필요 속에 정보보호 솔루션들에 대한 관심이 급격히 증가하고 있고, 그 도입 적용이 IT시스템을 운영하는 대부분의 기업, 기관들에게 있어 필수적으로 되어가는 상황이다. 그런 정보보호 니즈 속에 요즘 화두가 되고 있는 것이 바로 "통합"[7][8]이라고 할 수 있다.

정보보호 시장은 단순 보안제품의 구매/설치의 시장

"본 연구는 지식경제부 및 정보통신산업진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음"
(NIPA-2010-(C1090-1031-0001))

접수번호 : #100601-002
접수일자 : 2010년 06월 01일
심사완료일 : 2010년 07월 26일
교신저자 : 양해술, e-mail : hsyang@hoseo.edu

에서 체계적이고 효율적인 운영/관리의 시장으로 바뀌어 가고 있다. 성능 좋은 보안솔루션에 대한 관심과 다양화되고 전문적인 보안 솔루션들을 어떻게 체계적이고 운영관리 하느냐에 대한 문제가 대두되면서 각 보안제품에 대한 중앙집중적 통합관리에 대한 요구 즉, 방어 체계의 고도화에 따른 복잡도를 유지하면서 전문화된 관리의 단일화를 통해 보안서비스의 질을 높이기 위한 솔루션에 대한 새로운 니즈가 발생하고 있는 것이다.

ESM(Enterprise Security Management) 이란 방화벽, 침입탐지시스템(IDS), 가상시설망(VPN) 등 다양한 종류의 보안 솔루션을 하나로 모은 통합보안관리시스템이다. ESM은 최근 통합관리 수준에서 벗어나 시스템자원관리(SMS), 네트워크자원관리(NMS) 등 전사적 자원관리 시스템까지 포함하는 형태로 개발되는 추세여서 ESM 시장은 몇몇 업체를 제외하곤 상용화된 제품이 거의 없을 정도로 아직 개발 단계에 불과하며 체크포인트 등 주요 보안솔루션 업체들이 최근 보안솔루션 상호연동을 위한 표준 프로토콜(OPSEC)에 합의하면서 ESM 구현을 가속화하고 있다. ESM은방화벽, 침입탐지 시스템, VPN, 기타 보안제품에 대해서 특징을 가직 있으며, 침해 모니터링 관제현황 보고, 경보/대응 및 추적/분석, 정책관리, 성능관리 등에 관해 관리를 통합하는 역할을 한다. 이를 통해 인력, 시간, 투자비에 대해서 절약할 수 있는 장점을 가지고 있다. 이에 대한 내용이다음의 [그림 1]과 같다.

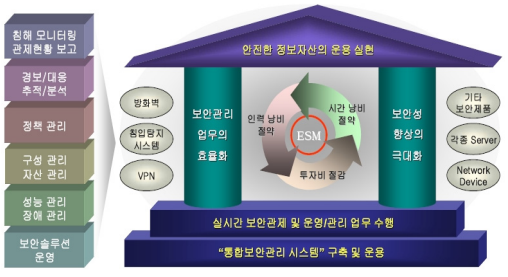

그림 1. ESM의 정의

본 연구에서의 ESM 소프트웨어의 품질평가 모델을 개발하는 것은 ESM 소프트웨어을 효과적으로 보호하기 위한 기초가 된다고 할 수 있다. 본 논문에서는 ESM 소프트웨어 분야 기반기술을 조사하고 ESM 소프트웨어 기술, 시장, 표준 및 시험·인증 동향을 조사하며 ESM 소프트웨어의 평가 모델을 개발하고자 한다. 즉, ESM 소프트웨어의 요구사항을 반영하여 시험 모듈을 개발하여 시험방법과 더불어 시험사례를 제안하였다.

2. ESM 소프트웨어 관련 연구

2.1 ESM의 필요성

인터넷 환경에서 발생되는 보안 침해 사고에 대응하기 위하여 대부분의 기업들은 전문 기능 위주의 다양한 보안 도구들을 순차적으로 도입하여 왔다.

지금까지 개별 솔루션 위주로 형성되고 온 보안 시장이 ESM 중심의 통합보안솔루션 중심으로 이동하고 있으며 이와 함께 PKI(Public Key Infrastructure) 분야는 완전한 거래 인프라를 확립하고 e커머스 활성화를 위한 인증의 핵심요소로 각광받을 것으로 전망되고 e메일 보안은 콘텐츠필터링, 암호화 서비스 등을 결합한 턴키 베이스 솔루션이 부각될 것으로 예상된다.

그러나, 사이버상의 위험은 지속적으로 변형/증가하여 그 대응 방안의 끝을 찾기 어렵게 되었고 더군다나 이제까지 산발적으로 도입 적용한 단위 보안 도구들을 전사적 보안 관리 측면에서 관리하는데 있어 다음과 같은 문제점들이 발생하게 되었다.

- 보안 도구/콘솔이 독립적인 운영 및 관리로 보안관리자의 생산성 저하
- 과도하게 발생하는 보안경보로 보안관리자의 보안 이벤트 중요성 인식 저하
- 다양한 단위보안 도구에서 발생하는 다량의 경보와 이벤트에 대한 연관성 파악 부재로 시스템이 어떤 위험에 노출되어 있는지 파악이 용이하지 않음.
- 단위보안 툴에서 발생하는 로그의 분산 저장으로 감사대비책 미비
- 침입탐지 솔루션의 최대 단점인 과도한 false alarm의 발생 및 로그의 발생으로 인해 보안 관리자들이

전체 단위솔루션들을 효율적으로 관리할 수 없음.

위와 같은 보안시스템 관리에 있어서의 현안들을 해결하고 효과적으로 운영하기 위해서는 개별 보안 솔루션을 중앙집중적으로 관리하며 각 보안제품에서 제공하는 정보들을 취합하여 상호 관련성을 정의하여 관리자에게 중요한 정보를 알려주고 전사적인 보안 정책을 일관성 있게 적용 관리할 수 있도록 하는 기능[9]을 갖는 통합보안관제시스템(ESM)의 도입이 필요하다고 말할 수 있다. 세계적인 IT기술 및 시장 동향 정보 제공기관인 가트너 그룹(www.gartner.com)도 통합보안관리솔루션(일종의 ESM)의 등장은 Falsealarm의 문제를 나타낸 기존 IDS(Intrusion Detection System)기술의 한계, 내/외부 위협과 정책 위반에 대해 전사적으로 파악하고 대응할 수 있는 일관된 방안의 부재, IT 보안 감사를 위한 문서/관리화의 부재 등의 이유 때문인 것으로 보고 있다.

2.2 ESM의 핵심기술

ESM은 시스템 하나로 다 각도의 보안관리를 할 수 있는 통합보안시스템이다. 통합보안시스템은 9가지의 보안관리가 이루어지고 특수 문 구축, 로비게이크 구축, 엘리베이터 통제, 방문객관리, IBS(Intelsat business service)연동(전력, 공조, 소방), 위치 추적 시스템, 재실관리 시스템, 순찰 관리 시스템, 외곽 보안 시스템이 바로 그것이다.

2.2.1 특수 문 구축

비 허가자가 출입 허가자를 뒤따라가는 동행출입을 방지하는 시스템이다. 센서가 내장되어 있어서 출입인원수를 체크하여 인증 인원수와 센서 인식 숫자가 일치하지 않으면 통행 중간 지역에서 갇히게 되는 시스템[10]이다. 뒤따라 들어가는 것만 방지되는 것이 아니라 장비 반출까지 방지되기 때문에 더 안심할 수 있다.

ESM은 ESM Server을 중심으로 관제센터, 원격 관리용 그리고 네트워크를 통해 여러 Agent를 관리하고 있다. 이에 대해서 [그림 2]와 같이 ESM 시스템의 구성을 나타냈다.

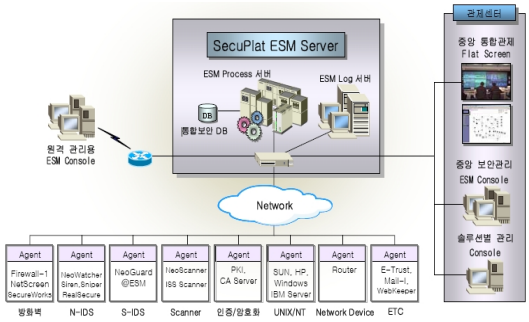

그림 2. ESM 시스템의 구성

2.2.2 로비게이트 구축

출입통제 시스템과 연동하여 출입 허가된 직원 및 방문자를 선별 출입시킴으로써 보안성을 강화시킨다. 방문객과 상주 근무 인원의 효율적인 출입관리가 이루어져 출입인원의 보안의식을 고취시킬 수 있다.

2.2.3 엘리베이터 통제

허가된 사람만 엘리베이터를 이용할 수 있도록 운영된다. 일반인 사용이 금지된 엘리베이터에 RF 리더기를 설치해서 일반인이 탑승할 경우 층 버튼이 동작하지 않게 해놓았다. 만일 강압으로 인해 침입자와 허가자가 같이 탑승했을 경우 침입자 모르게 중앙 통제실에 상황을 전달해서 사고에 신속히 대응한다.

2.2.4 방문객 관리시스템

건물의 출입구나 보안이 필요한 특수 지역에 검색대를 설치해서 무기류 및 각종 흉기 소지자를 색출할 수 있다. 방문자는 반드시 신분증과 방문 출입증을 교환하여 출입하기 때문에 사고 발생시 추적할 수 있도록 데이터를 관리한다.

2.2.5 IBS 연동 시스템

조명, 공조, 소방 시스템에서 연동하여 운영이 되는데 조명은 최초 출근자가 사무실에 입실하면서 조명이 켜지고 최종 퇴실자가 사무실 퇴실하면 조명이 꺼진다. 이들의 데이터를 이용하여 에어컨이나 히터의 작동도 함께 이루어지고 화재 발생시에는 전체 출입문 및 그룹별 출입문이 자동 개방된다.

2.2.6 위치 추적시스템

RF 태그를 이용하여 사람이나 물체의 이동을 추적할 수 있고 긴급 상황이 발생하면 실시간으로 대응이 가능해서 편리하다. 외부인에 대한 정확한 동선 파악으로 보안성을 강화하였다.

3. ESM의 동향

통합보안관리솔루션은 여러 문제들의 극복 및 전사적 보안 관리 체계의 확보를 위해 보아 장비 및 솔루션들의 통합 관리뿐 아니라 네트워크 및 시스템들의 보안 정보들 그리고 더 나아가서는 Application, Transaction, Business 입장에서의 보안 정보를 통합관리하는 통합보안관리체계로 확장 발전할 것으로 예측하고 있다.

보안 선진국이라고 일컫는 미국 본토에서 아직 ESM에 대한 정확한 개념이 자리 잡지 않은 상태지만 ESM은 통합보안관리를 위한 워크플로우(Workflow)관점에서 이해하는 것이 가장 적합할 것 같다. 특히 최근의 동향을 분석해 보면 ESM이 보안 관리를 위한 워크플로우의 모습을 보이고 있다. 즉 보안정책을 수립하고 수립된 보안정책에 따라 시스템을 구현하며, 이를 모니터링 하거나 신속하고 효과적인 조치를 위해 각종 경보 기능을 제공하는 등 일련의 워크플로우를 일관되게 지원하는 것이 그것이다. 흔히 말하는 ESM이란 Enterprise Security Management, 즉 전사적 통합보안관리를 일컫는데 전통적으로 ESM은 IT 인프라 환경 관점에서 보았을 때 다음의 두 가지 영역에 초점[11]을 맞추고 있다고 할 수 있다.

3.1 User Administration과 Management

보안 또는 정책관리에 따른 사용자 및 Access관리에 무게중심을 두고 있는 범주이다. 이 범주에는 인증이나 Single Sign-On의 기능을 포함하는 경우가 많다. 이러한 유형에는 초기 ESM개념이 많이 반영되어 있어 보안적인 측면보다는 시스템 관리적 성격이 짙다고 볼 수 있다.

3.2 취약점분석이나 위험평가 등의 Risk Assessment

네트워크 및 시스템의 취약점, 위험 요소들을 분석하고 모니터링하는 관리도구의 형태를 취하여 제품에 따라 분석 또는 정책관리, 모니터링 및 경보(Alert)등 어느 쪽에 무게를 두느냐에 따라 약간씩 특성을 달리 하고 있다. 최근에 출시된 ESM 제품의 주류를 이루고 있으며 기존 보안 제품들과의 통합(Integration)이 활발히 진행되고 있는 범주에 속한다.

따라서 최근의 ESM 추세로 보면 ESM은 네트워크나 시스템 리소스들의 각종 위험요소들을 분석하고 모니터링하는 일종의 '관리 도구'로서 침입차단시스템, 침입탐지시스템, 안티바이러스 제품 등 기존의 멀티벤더 보안 솔루션들을 통합 관리함으로서 관리의 효율성[12][13]을 높이고 능동적인 보안대책을 세울 수 있도록 도와주는 보안관리 도구라고 할 수 있을 것이다.

4. ESM 소프트웨어의 품질특성 시험 모듈

이 절에서는 ESM 소프트웨어의 각 품질특성에 대한 품질평가의 기반이 되는 평가 요소를 확립하였다.

본 논문에서 제시한 평가항목들은 지식정보보안 제품 중 ESM 제품의 특성을 고려하고 제품의 일반 품질 요구사항으로 커버되는 품질 요소와 ESM 제품의 고유한 품질 요구사항을 도출하여 지식정보보안 제품의 주요 특성인 보안성 및 보안성능을 심도 있게 평가할 수 있도록 하였다.

즉, 기존의 품질평가 모델에서 충분히 고려되지 않아 한계로 지적되었던 제품별 품질평가 모델을 제시하였으며, 기존의 정보보호 제품에 대한 CC(Common Criteria) 인증이 보안기능과 취약성 중심의 평가를 함으로써 제대로 다루어 지지 않았던 특성들을 포괄적으로 적용할 수 있는 품질평가 모델을 구축하였다.

본 연구에서는 품질 수준 지표를 소프트웨어 제품평가를 위한 국제표준인 ISO/IEC 9126[1]과 소프트웨어 시험에 관한 지침인 ISO/IEC 12119를 기반으로 하여 구축하였다. 즉, 주특성 6가지의 부특성에 대한 시험모

듈에 일부가 [표 1]-[표 6]과 같다.

4.1 기능성에 관한 품질수준 지표

국제표준인 ISO/IEC 9126과 소프트웨어 시험에 관한 지침인 ISO/IEC 12119를 기반으로 기능성의 5가지 부특성에는 지정된 작업과 사용자 목적을 위한 적절한 기능들을 제공하는 제품의 능력을 말하는 적합성, 요구하는 정밀도를 유지하도록 결과 값을 제공할 수 있는 제품의 능력을 말하는 정확성, 제품 또는 시스템과 상호작용 할 수 있는 상호운영성, 준수성 중에 적합성에 관한 시험모듈은 [표 1]과 같다.

표 1. 적합성 시험모듈

메트릭명	기능 정보 제공	계산식	기능 정보 제공 = B(문서에 언급된 기능 수)/A(프로그램에서 제공하는 모든 기능 수)
		결과 영역	0 ≤ 기능 정보 제공 ≤ 1
	경계값 정보 제공	계산식	경계값 정보 제공 = B(문서에 설명된 경계값 항목의 수)/A(프로그램 사용에 필요한 모든 경계값 항목의 수)
		결과 영역	0 ≤ 경계값 정보 제공 ≤ 1
	경계값 처리율	계산식	- 경계값 처리율 = B(각 항목별 테스트케이스 성공률의 합)/A(경계값 확인 대상 항목 수) - B= $\sum_{i=1}^{A} \frac{Success\_TC_i}{Total\_TC_i}$ - Success_TC : i 번째 경계값 처리 기능 확인을 위해 수행한 테스트케이스 중 성공한 건 수 - Total_TC : i 번째 경계값 처리 기능 확인을 위해 수행한 테스트케이스 수
		결과 영역	0 ≤ 경계값 처리율 ≤ 1

4.2 신뢰성에 관한 품질수준 지표

국제표준인 ISO/IEC 9126과 소프트웨어 시험에 관한 지침인 ISO/IEC 12119를 기반으로 신뢰성의 4가지 부특성에는 제품 내의 결함으로 인한 장애를 피해 가는 제품의 능력을 의미하는 성숙성, 제품 결함이 발생했을 때 명세된 성능 수준을 유지 할 수 있는 오류허용성, 데이터를 복수하는 제품 능력을 의미하는 회복성, 준수성 중 성숙성에 관한 시험모듈은 [표 2]와 같다.

표 2. 성숙성 시험모듈

메트릭명	문제 해결 이력 정보 제공	계산식	- 문제해결이력 정보제공 = A(문제해결 이력 정보 제 공 여부)
		결과 영역	문제해결이력 정보제공 = Y or N or NA
	문제 해결률	계산식	문제해결률 = B(확인된 문제 해결 항목수)/A(시험 대상 문제 해결 항목수)
		결과 영역	0 ≤ 문제해결률 ≤ 1
	결함 회피율	계산식	결함 회피율 = 1- min(1, B(발견된 결함 수)/A(단위 운용시간))
		결과 영역	0 ≤ 결함 회피율 ≤ 1

4.3 효율성에 관한 품질수준 지표

국제표준인 ISO/IEC 9126과 소프트웨어 시험에 관한 지침인 ISO/IEC 12119를 기반으로 효율성의 3가지 부특성에는 명시된 조건에서 그 기능을 수행할 때 적절한 반응 및 처리 시간과 처리율을 제공하는 제품의 능력을 의미하는 시간효율성과 적절한 자원을 사용하는 제품의 능력인 자원 효율성, 준수성 중에서 시간효율성에 관한 시험모듈은 [표 3]과 같다.

표 3. 시간효율성 시험모듈

메트릭명	평균 반응 시간	계산식	- 평균반응시간 = 1- min (1, B(반응 평균시간)/A(반응평균시간의 한계값)) - B = $\frac{\sum_{i=1}^{n} T_i}{N}$ - Ti = i 번째의 테스트의 반응시간 - N= 반응시간 테스트 케이스 수
		결과 영역	0 ≤ 평균 반응 시간 ≤ 1

4.4 사용성에 관한 품질수준 지표

국제표준인 ISO/IEC 9126과 소프트웨어 시험에 관한 지침인 ISO/IEC 12119를 기반으로 사용성의 5가지 부특성에는 제품이 적합한지 특정 작업과 사용조건에서 어떻게 사용될 수 있는지를 사용자가 이해할 수 있도록 하는 이해 가능성, 제품이 제공하는 기능을 학습할 수 있도록 하는 학습 가능성, 사용자가 제품을 운영하고 제어할 수 있도록 하는 운영성, 사용자에 의해 선호되는 제품의 능력인 선호도 그리고 준수성 중 이해가능성에 관한 시험모듈은 [표 4]와 같다.

표 4. 이해가능성 시험모듈

메트릭명	기능 이해도	계산식	기능 이해도 = A(제품설명서와 사용자 문서를 통해 이해할 수 있는 기능의 수)/B(전체 기능의 수)
		결과 영역	0 ≤ 기능 이해도 ≤ 1
	인터페이스 이해도	계산식	인터페이스 이해도 = A(인터페이스를 통하여 이해할 수 있는 기능의 수)/B(전체 기능의 수)
		결과 영역	0 ≤ 인터페이스 이해도 ≤ 1

4.5 유지보수성에 관한 품질수준 지표

국제표준인 ISO/IEC 9126과 소프트웨어 시험에 관한 지침인 ISO/IEC 12119를 기반으로 유지보수성의 5가지 부특성에는 제품의 결함이나 장애의 원인 또는 변경될 부분들의 식별에 대한 진단을 가능하게 하는 분석성과 특정 변경요구사항이 시스템에 반영될 수 있게 하는 변경성, 제품의 설정 변경으로 인한 예상치 않은 결과를 최소화하는 안전성, 테스트 용이성, 준수성이 있다. 이 중 분석성에 관한 시험모듈은 [표 5]와 같다.

표 5. 분석성 시험모듈

메트릭명	진단 기능 정보 제공	계산식	진단기능 정보제공 = A(진단기능에 관한 정보 제공 여부)
		결과 영역	진단기능 정보 제공 = Y or N or NA
	진단 기능 지원률	계산식	– 진단기능 지원 = B(각 항목별 테스트케이스 성공률의 합)/A(평가할 진단기능의 수) – $B = \sum_{i=1}^{A} \frac{Success\_TC_i}{Total\_TC_i}$ – Success_TC : i 번째 진단기능 확인을 위해 수행한 테스트케이스 중 성공한 건 수 – Total_TC : i 번째 진단기능 확인을 위해 수행한 테스트케이스 수
		결과 영역	0 ≤ 진단기능 지원 ≤ 1

4.6 이식성에 관한 품질수준 지표

국제표준인 ISO/IEC 9126과 소프트웨어 시험에 관한 지침인 ISO/IEC 12119를 기반으로 이식성의 5가지 부특성에는 제품이 특정 환경에서 다른 환경으로 적응할 수 있는 능력인 적응성, 명세된 환경에서 설치될 수 있는 설치가능성, 동일한 환경에서 동일한 목적으로 지정된 제품을 대신하녀 사용될 수 있는 대체성, 공통자원을 공유하는 공동 환경에서 다른 독립적인 제품과 공존할 수 있는 공존성, 준수성이 있다. 이 중 적응성에 관한 시험모듈은 [표 6]과 같다.

표 6. 적응성 시험모듈

메트릭명	데이터 구조 적응 정보 제공	계산식	데이터구조 적응 정보제공 = A(데이터 구조 적응에 관한 정보 제공 여부)
		결과 영역	데이터구조 적응 정보제공 = Y or N or NA
	데이터 구조 적응률	계산식	– 데이터구조 적응률 (DAR) = B(각 항목별 테스트케이스 성공률의 합)/A (평가할 데이터구조 적응시킬 데이터 항목 수) – $B = \sum_{i=1}^{A} \frac{Success\_TC_i}{Total\_TC_i}$ – Success_TC : i 번째 데이터 항목 확인을 위해 수행한 테스트케이스 중 성공한 건 수 – Total_TC : i 번째 데이터 항목 확인을 위해 수행한 테스트케이스 수
		결과 영역	0 ≤ 데이터구조 적응률 ≤ 1

5. ESM 소프트웨어의 시험평가

5.1 시험을 위한 환경 구축

본 연구에서 시험한 ESM 소프트웨어는 기업내의 관리 대상 클라이언트에 설치된 안티 바이러스 프로그램을 업데이트 및 관리하는 안티 바이러스 통합관리 프로그램으로 주요 기능은 서버 : 접근제어 설정, 보조서버 설정, DB 설정, 로그관리, 관리자 설정 등이 있으며, 콘솔 : 정책 관리, 노드 관리, 명령 수행, 사이트 관리 등, 에이전트 : 정책 적용, 엔진 업데이트, 실시간 감시기 제어, 메시지 전송 등이 있다. ESM 소프트웨어의 시험 환경 구축은 [그림 3]과 같이 구축 하였다.

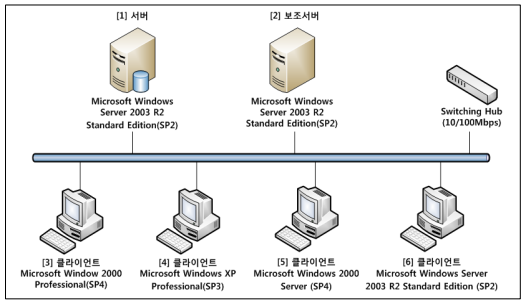

그림 3. 시험 환경의 구축

ESM 소프트웨어의 [1]번 서버에 설치한 프로그램으로는 시험 대상 제품(서버 모듈, 콘솔 모듈), DBMS: Microsoft SQL Server 2005, 일반 응용프로그램: Microsoft Office 2007, 한글 2005 등이며, [2]번 보조서버에 설치한 프로그램으로는 시험 대상 제품(서버 모듈, 콘솔 모듈), 일반 응용프로그램: Microsoft Office 2007, 한글 2005 등을 설치하였으며 [3]-[6]번 클라이언트에 설치한 프로그램은 시험 대상 제품(에이전트 모듈)과 일반 응용프로그램: Microsoft Office 2007, 한글 2005 등을 설치하였고 네트워크에는 10/100/1000Mbps 스위칭 허브를 사용하였다. 성능측정을 위한 성능측정 도구는 Performance Logs and Alerts를 [1]번 서버와 [3]-[6]번 클라이언트에 설치하였다.

5.2 결함내역 및 속성분석

ESM 소프트웨어 시험평가를 한 후 결함 내역과 속성에 대해서 분석하였다.

5.2.1 결함 내역

"ESM 소프트웨어의 품질특성 시험 모듈"에서 제시한 메트릭을 바탕으로 [그림 3]의 시험환경에서 시험한 결과 나타난 결함을 품질특성 및 결함속성별로 ESM 소프트웨어에 대한 5종류의 사례를 결함 건수 및 내역 등을 정리하면 [표 7]과 같다.

표 7. ESM 소프트웨어의 결함 내역

품질특성	수정전 결함수	최종 결함수
기능성	42	0
신뢰성	4	0
효율성	0	0
사용성	67	1
유지보수성	2	0
이식성	0	0
일반적 요구사항	0	0
계	115	1

5.2.2 결함속성 분석

(1) 기능성

ESM 소프트웨어의 기능성 결함을 살펴보면 다음과 같은 정책 설정 기능, 실시간 하드웨어 정보 얻기 기능, 악성코드 감염현황 표시 기능, 클라이언트 정보 표시 기능, SW/파일 배포 기능, 업데이트 기능 등에서 결함이 발생하였으나, 수정 보완 및 회귀시험 과정을 거친 후 최종적으로 제품에서 제공하는 기능이 정상 동작함을 확인하였다.

(2) 신뢰성

신뢰성 결함을 살펴보면 콘솔의 관리 트리에서 노드가 삭제되면 해당 클라이언트가 접속을 시도할 때까지 클라이언트를 관리할 수 없으나, 노드 삭제 시 경고 메시지를 제공하지 않는 결함과, 콘솔의 언어를 한국어에서 영어로 변경하면 일부 정보(예: 설치배포 메뉴의 유효 노드 접속일)가 삭제되는 등의 신뢰성 결함이 발생하였으나, 수정 보완 및 회귀시험 과정을 거친 후 최종적으로 정상 동작함을 확인하였다.

(3) 효율성

효율성 결함을 살펴보면 다음과 같다. 명시된 시험환경(하드웨어 및 소프트웨어, 네트워크 환경)에서 제품 운영시 CPU 사용률, 메모리 사용량은 서버 서비스를 구동시키는 경우, 서버의 CPU 사용률은 42.97%까지 올라갔지만 처리완료 후 1% 미만으로 내려갔다. 메모리 사용량은 550MB 이하로 일정하게 유지되었으며, 에이전트 서비스를 구동시키는 경우, 클라이언트의 CPU 사용률은 [4]번 클라이언트에서 최고 4.30%까지 올라갔지만 처리완료 후 모든 클라이언트에서 1% 미만으로 내려갔다. 메모리 사용량은 400MB 미만으로 일정하게 유지되었고, 서버에서 다수의 클라이언트로부터 1,000개, 2,000개, 3,000개의 바이러스 이벤트 로그를 수집하는 경우, 서버의 CPU 사용률은 각각 30.86%, 54.30%, 63.67%까지 올라갔지만 처리완료 후 모두 1% 미만으로 내려가고, 메모리 사용량은 590MB 미만으로 일정하게 유지되었다.

(4) 사용성

사용성 결함을 살펴보면 콘솔 및 에이전트의 로그에 출력되는 시간표시 형식에 일관성이 미흡하였고, 콘솔의 '악성코드 예방' 항목 변경 시 제공되는 '적용(A)'버

튼의 단축키와 '고급(A)'메뉴의 단축키가 동일하였으며, 에이전트 삭제 시 팝업되는 메시지가 영문으로 제공되는 등의 사용성 결함이 발생하였으나, 수정 보완 및 회귀시험 과정을 거친 후 최종적으로 수정 되었음을 확인하였다.

(5) 유지보수성

유지보수성의 결함을 살펴보면 제품 구동 중 발생하는 로그파일의 경로 정보를 제공하지 않았고, 유지보수에 필요한 정책 동작 정보가 제공되지 않는 등의 유지보수성 결함이 발생하였으나, 수정 보완 및 회귀시험 과정을 거친 후 최종적으로 수정 되었음을 확인하였다.

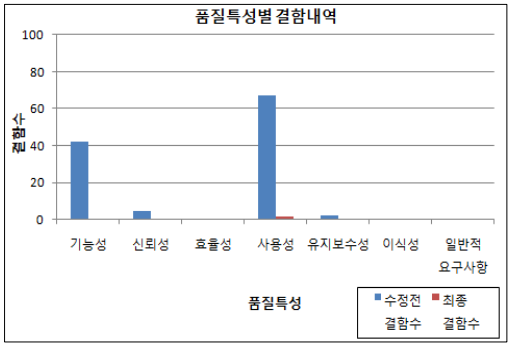

그림 4. 품질특성별 결함내역

[그림 4]에서는 품질 특성별 결함 내역을 나타낸 그래프이다. 주특성 사용성이 가장 많은 결함 내역이 나타나고 있는 것을 알 수 있으며, 그 뒤로는 기능성의 결함 내역이 높은 것을 알 수 있다.

5.3 성능시험

5.3.1 성능시험 시나리오

표 8. 성능시험 시나리오

시나리오ID	설명
SC_1	서비스를 구동 ※ 서버에서 서버 서비스 구동, 클라이언트에서 에이전트 서비스 구동
SC_2	서버에서 다수의 클라이언트로부터 바이러스 이벤트 로그를 수집 ※ 이벤트 로그 개수: 1,000개, 2,000개, 3,000개

ESM 소프트웨어의 성능시험 시나리오를 살펴보면 SC_1에서는 서버에서 서버 서비스 구동, 클라이언트에서 에이전트 서비스 구동시키고 SC_2에서는 서버에서 다수의 클라이언트로부터 바이러스 이벤트 로그를 수집하였다.

5.3.2 측정항목

ESM 소프트웨어 성능시험에서의 측정항목을 살펴보면 CPU사용률과 메모리 사용량으로 나누어 측정하였으며 CPU사용률은 비유휴 스레드를 실행하는데 소비하는 시간의 백분율을 측정하였고 메모리 사용량은 시스템에서 실행되고 있는 프로세스에 할당되어 사용된 메모리의 양을 측정하였다.

표 9. 측정항목

항목	단위	내용	
CPU 사용률	%	%Process or Time	비유휴 스레드를 실행하는데 소비하는 시간의 백분율
메모리 사용량	MB	Private MBytes	시스템에서 실행되고 있는 프로세스에 할당되어 사용된 메모리의 양

5.4 성능시험결과

성능 시험은 자원효율성을 측정하였으며, 결과는 다음과 같다.

5.4.1 자원 효율성

(1) CPU 사용률

- 서버 서비스를 구동시키는 경우, 서버의 CPU 사용률은 42.97%까지 올라갔지만 처리완료 후 1% 미만으로 유지됨
- 에이전트 서비스를 구동시키는 경우, 클라이언트의 CPU 사용률은 [3], [4], [5], [6]번 클라이언트에서 각각 3.91%, 4.30%, 2.34%, 3.52%까지 올라갔지만 처리완료 후 모두 1% 미만으로 유지됨
- 서버에서 다수의 클라이언트로부터 1,000개, 2,000개, 3,000개의 바이러스 이벤트 로그를 수집하는 경우, 서버의 CPU 사용률은 각각 30.86%, 54.30%, 63.67%까지 올라갔지만 처리완료 후 모두 1% 미

만으로 유지됨

(2) 메모리 사용량
- 서버 서비스를 구동시키는 경우, 서버의 메모리 사용량은 541~550MB로 일정하게 유지됨
- 에이전트 서비스를 구동시키는 경우, 클라이언트의 메모리 사용량은 [3], [4], [5], [6]번 클라이언트에서 각각 280~285MB, 391~397MB, 384~389MB, 391~395MB로 일정하게 유지됨
- 서버에서 다수의 클라이언트로부터 1,000개, 2,000개, 3,000개의 바이러스 이벤트 로그를 수집하는 경우, 서버의 메모리 사용량은 각각 583~584MB, 578~580MB, 583~586MB로 일정하게 유지됨

5.5 평가방법의 비교분석

[표 10]의 ISO/IEC 9126과 ISO/IEC 12119 기반의 품질평가에 대한 장단점과 기존의 평가 방법에 대해 기술하고 비교하였다. ISO/IEC 9126은 ISO/IEC 9126-2의 외부메트릭에 의한 평가와 ISO/IEC 9126-3의 내부메트릭에 의한 평가로 분류할 수 있다. 외부메트릭에 의한 평가는 국제표준을 기반으로 하여 상대적으로 높은 객관성을 가지며 실행 프로그램의 평가에는 적합하지만 라이프사이클 전반에 적용할 수 없다. 내부메트릭에 의한 평가는 높은 객관성을 가지며 실행 프로그램에 한정되지 않고 소프트웨어 개발 전 과정의 중간산출물 대상으로 하여 소프트웨어 라이프사이클 전반에 걸쳐 적용할 수 있지만 중간산출물의 품질 측정을 통해 최종 소프트웨어 제품인 실행 프로그램의 품질을 예측하는 수준에 그칠 뿐 확신할 수 없다는 단점이 있다.

ISO/IEC 12119 기반의 품질평가 방법의 경우에는 국제표준을 기반으로 하여 객관성을 확보할 수 있으며 소프트웨어의의 다수를 차지하는 패키지 소프트웨어의 평가에 적합하지만 기본적인 표준만으로는 일반적인 사무용 패키지 소프트웨어 중심으로서 다양한 소프트웨어 분야에 적용하기 쉽지 않다.

본 연구의 평가 방법은 ISO/IEC 9126과 12119를 기반으로 ESM 소프트웨어에 초점을 맞추어 핵심적이고 최적화된 평가가 가능하지만 범용적인 품질평가 표준을 기반으로 하여 ESM 소프트웨어의 특성을 수용하여 구체화하였으므로 ESM 소프트웨어 고유의 특성에 대한 반영이 미흡할 수 있으므로 향후, ESM 소프트웨어의 관련 표준을 프레임워크로 한 품질평가 방법에 대한 연구가 추진되어야 할 것으로 생각된다.

표 10. 품질평가 방법의 비교

평가방법 \ 구분		장점	단점	비고
ISO/IEC 9126 기반의 평가방법	외부 메트릭 기반	국제표준을 기반으로 하여 상대적으로 높은 객관성을 가지며 실행 프로그램의 평가에 적합	실행 프로그램을 대상으로 평가하는데 한정되므로 라이프사이클 전반에 적용할 수 없음	
	내부 메트릭 기반	높은 객관성을 가지며 실행 프로그램에 한정되지 않고 S/W 개발 전 과정의 중간산출물 대상으로 함	중간산출물의 품질로 실행 프로그램의 품질을 예측하나 확신할 수 없음	
ISO/IEC 12119 기반의 품질평가 방법		국제표준을 기반으로 하여 높은 객관성을 가지며 S/W의 다수를 차지하는 패키지 S/W 평가에 적합	일반적인 사무용 패키지 S/W 중심으로서 다양한 S/W 분야에 적용하기 쉽지 않음	평가대상S/W의확대를위한 연구활발
본 연구의 평가방법		ISO/IEC 9126과 12119를 기반으로 ESM S/W의 이식성에 초점을 맞추어 핵심적이고 최적화된 평가 가능	범용적인 품질평가 표준을 기반으로 ESM S/W의 특성을 수용하여 구체화하였으므로 고유의 특성에 대한 반영이 미흡할 수 있음	

6. 결 론

본 연구 시험하였던 제품은 기업내의 관리 대상 클라이언트에 설치된 안티 바이러스 프로그램을 업데이트 및 관리하는 안티 바이러스 통합관리 프로그램으로, 제공된 기능이 정확히 동작하는지, 제품을 장시간 운영하였을 때 기능 및 성능상의 문제가 발생하지 않는지, 다수의 바이러스 발견으로 인한 이벤트 발생 시에도 제품 운용이 원활한지, 사용자를 위한 설명서 내용은 충실한지, 유지보수는 용이한지 등을 중점적으로 평가하였다. 그리고 국제품질표준 ISO/IEC 9126을 기반으로 ESM 소프트웨어의 품질 평가 모델을 개발하고 평가 과정에서 활용할 수 있는 품질검사표를 개발하였으며 시나리오를 작성해 성능시험을 테스트한 결과를 통하여 자원

효율성과 시간효율성을 측정하는 방안을 모색하였다. 또한, ESM 소프트웨어의 품질평가 방법을 구축하여 품질 수준의 제고를 위한 기준을 제시하였다. ESM 소프트웨어의 품질평가 모델 개발과 향후 실질적인 활용을 통해 ESM 소프트웨어의 품질수준을 향상시킬 수 있다고 본다.

참 고 문 헌

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

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

[3] Fan Chen and Ravi S, Sandhu. Constrainsts for Role-based Access control, George Mason University, 1996.

[4] Mimicry Attacks on Host Based intrusion Detection System. David Wagner. Paolo Soto, 2003.

[5] ISO/IEC 14598-1 : 1999, Information technology - Software product evaluation - Part 1: General overview.

[6] ISO/IEC 14598-2 : 2000, Software engineering - Product evaluation - Part 2: Planning and management.

[7] Ehab Al-Shaer and Hazem Gaqmed, "Discovery of Policy Anomalies in Distributed Firewalls" in Proc. of IEEE INFOCOMM' 04. Vol 23.

[8] 이영석, 나중찬, 손승원, ESM 개발동향:이기종 보안 시스템 연도을 중심으로, IITA 기술정책정보단, 2003(5).

[9] 정연서, 류걸우, 장종수, "네트워크 보안을 위한 ESM 기술 동향", 한국전자통신연구원, 주간기술동향 통권 1026호, 2001(12).

[10] 이대식, 윤동식, 안희학, "ESM 시스템을 이용한 안정된 학내망 구축", 정보보증논문지, 제 5권, 제 3호, 2005(9).

[11] 김성락, "통합 보안 관리 에이전트를 확장한 웹 어플리케이션 공격 탐지 연구", 한국 컴퓨터정보학회 논문지, 제12권, 제1호, 2007(3).

[12] 최대수, 이용균, "ESM에서 보안이벤트 분석기술에 관한 연구", 한국컴퓨터종합학술대회 논문집, Vol.34 No.1(D), 2007.

[13] 이경화, "*능동형 통합보안관리 시스템 구조 설계*", 숭실대 정보과학대학원 석사논문, 2006(12).

저 자 소 개

강 득 수(Deuk-Soo Kang) 정회원

- 1975년 2월 : 중잉대학교 졸업(학사)
- 2007년 2월 : 호서대학교 벤처전문대학원 졸업(경영학석사)
- 2009년 3월 ~ 현재 : 호서대학교 벤처전문대학원 정보경영학과 박사과정
- 2005년 8월 : 서울대학교 경영대학원 최고경영자과정 수료
- 1975년 1월 ~ 1987년 3월 : LG전자 연구소 재직
- 1987년 4월 ~ 2001년 4월 : 기라정보통신(주) 법인설립 및 대표이사/회장
- 1999년 3월 ~ 2005년 12월 : (주)이레C&D 법인설립 회장
- 2000년 4월 ~ 현재 : (주)케이엠아이티 법인설립 대표이사
- 2002년 1월 ~ 현재 : 세일전자(주) 회장

<관심분야> : 품질경영 및 기업정보관리, 프로젝트관리 및 컨설팅, 기업통합관리 컨설팅, S/W 품질보증과 평가

양 해 술(Hae-Sool Yang) 정회원

- 1975년 2월 : 홍익대학교 전기공학과 졸업(학사)
- 1978년 8월 : 성균관대학교 정보처리학과 졸업(석사)
- 1991년 3월 : 日本 오사카대학 정보공학과 SW공학(공학박사)
- 1975년 5월 ~ 1979년 6월 : 육군중앙경리단 전자계산실 시스템분석장교
- 1980년 3월 ~ 1995년 5월 : 강원대학교 전자계산학과 교수
- 1986년 12월 ~ 1987년 12월 : 日本 오사카대학교 객원연구원
- 1995년 6월 ~ 2002년 12월 : 한국SW품질연구소장
- 1999년 11월 ~ 현재 :호서대학교 벤처전문대학원 교수
- 2010년 3월 ~ 현재 : 호서대학교 글로벌창업대학원장

<관심분야> : SW공학(특히, SW 품질보증과 품질평가, 품질감리 및 컨설팅, OOA/OOD/OOP, SI), SW 프로젝트관리, 품질경영