기업보안관리(ESM) 제품의 보안성 평가모델 및 시험방법론 개발

Development of Security Evaluate Model and Test Methodology of Enterprise Security Manageent (ESM) Product

차영환*, 양해술**
서울벤처정보대학원대학교*, 호서대학교**

Young-Hwan Cha(yhcha@kdb.co.kr)*, Hae-Sool Yang(hsyang@hoseo.edu)**

요약

국내에선 ESM(Enterprise Security Management)이 보안관리를 대표하고 있고, 이를 더욱 고도화해야 한다는 요구가 증가하고 있다. 본 논문에서는 기업보안관리(ESM) 제품의 질적인 면을 평가하고 품질 수준을 파악하여 개선방향을 도출함으로써 품질향상을 지원할 수 있는 보안성 평가모델과 시험 방법론에 대해서 개발하였다. 그리고 제품의 보안성 품질을 측정하고 그 결과를 적절한 기준에 따라 판정하는 방법에 대해 연구를 수행하고자 성능시험사례를 제시하여 평가방법을 제시하였다. 도출된 품질평가 모델은 침입방지 시스템의 품질을 평가하고 향상시키는데 중요한 역할을 하게 될 것으로 기대한다.

■ 중심어 : | ESM | 보안성 | 평가모델 |

Abstract

ESM(Enterprise Security Management) is representing domestic security management, and there is requirement to enhance it. This paper will evaluate quality of ESM products, understand its quality level, and derive method to improvement so as to develop security evaluation model and test methodology which can support quality enhancement. In addition, it presented the performance test cases and evaluation method to measure product's security quality, and to perform research on the judgement method for the results based on appropriate criteria. Developed quality evaluation model is expected perform important role in evaluating and enhancing the quality of intrusion prevention system.

■ keyword : | ESM | Security | Evaluate Model |

Ⅰ. 서 론

ESM이란 Enterprise Security Management의 약자로서, 국내 정보보호 업계에서 통용되는 용어이지만 학술 연구 단체 또는 산업 표준단체 등에 의해 정의되고 명세화된 후 업계에서 통용된 것이 아니기 때문에, 그 의미 및 요구 기능에 있어서 정보보호 업체 및 소비자 또는 학계 및 산업계에서 다양한 관점으로 접근되고 있다. 이를 관점의 차이는 통합의 범위, 관리의 해석 범위에 따른 것이라고 할 수 있다.

그러나, 일반적으로는 ESM이란 보안 시스템들을 하나의 통합 관리하고 유사한 보안 정책을 통일하여 적용하고 상호간의 연관분석을 통해 각 보안 시스템들의 상호 운용성, 관리성 및 보안성을 최대화하여 위험요소를

"본 연구는 지식경제부 및 정보통신산업진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음"
(NIPA-2010-(C1090-1031-0001))
접수번호 : #100309-005
접수일자 : 2010년 03월 09일
심사완료일 : 2010년 06월 01일
교신저자 : 양해술, e-mail : hsyang@hoseo.edu

최소화하는 관리 솔루션이라고 이해할 수 있다[5][6].

현재 구축되고 있는 대부분의 ESM시스템들은 이질적인 네트워크 환경에서 여러 업체가 제작한 다양한 종류의 보안 시스템들을 통합적으로 관리하는 이기종 보안장비 통합관리 기능과 시스템 및 네트워크 자원현황을 모니터링하는 IT자원 보안 모니터링 기능을 제공함으로써 고객사의 모든 전산 자원의 가용성 관리 및 보안성 관리 기능을 기본적으로 제공한다.

현재, IT(Information Technology)를 기반으로 하지 않은 비즈니스는 없다고 해도 과언이 아닐 정도로, 대부분의 비즈니스업무는 물론 일상생활까지 모두 컴퓨터 시스템의 도움을 받아 처리되고 있는 이즈음에 더구나, 정보 공유성을 극대화하기 위해 인터넷을 매개로 하는 개방형 네트워크 컴퓨팅 환경이 일반화 된 현재는 열린 환경 속에서 개인적인 정보 자산을 지키기는 일이 무엇보다 중요하다[7].

이런 정보자산을 지키기 위해 여러 기업들은 여러 보안 제품을 요구하기 시작하였다. 여러 기업의 요구에 보안 장비는 많은 장비들이 나왔으며 앞으로도 정보보안 제품의 시장은 지속적으로 성장할 것으로 예상된다. 이 시점에서 이에 따른 정보보안 제품의 품질 평가 요구에 대응하기 위하여 기업보안관리 제품의 품질 평가 모델 개발이 시급하다고 볼 수 있다.

본 논문은 크게 3가지 방향으로 구분하여 진행하였다.

첫째, 기업보안관리(ESM)의 특징, 시장 및 기술동향에 대해서 조사 및 분석하였다. 이는 기업보안관리(ESM)제품의 품질 평가 모델의 개발을 위해서 기업정보보안(ESM) 기술 체계를 정의하고 특성을 분석하여 품질평가 모델을 작성하는데 활용하였다. 그리고, 둘째, 기업보안관리(ESM)제품의 보안성 품질 평가기준을 도출하였다. 셋째, 도출된 기업보안관리(ESM)제품의 보안성 품질 평가기준을 가지고 평가방법 메트릭을 개발하였다.

II. 관련 연구

1. 기업보안관리 시스템의 특성

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 주요 보안솔루션 업체들이 최근 보안솔루션 상호연동을 위한 표준 프로토콜에 합의하면서 ESM 구현을 가속화하고 있어 국내에서도 데이터게이트, 이글루시큐리티, 인텐, 어울림정보기술 등 보안업계들이 최근 ESM을 잇따라 출시하면서 제품 상용화에 주력하고 있다[10][11].

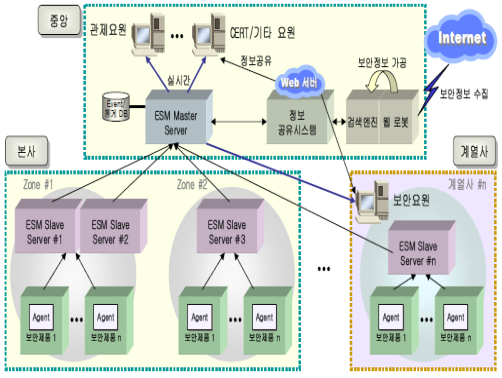

그림 1. ESM 구축 유형

이에 따라 지금까지 개별 솔루션 위주로 형성되어 온 보안 시장이 ESM 중심의 통합보안솔루션 중심으로 이동하고 있으며 이와 함께 PKI분야는 완전한 거래 인프라를 확립하고 e커머스 활성화를 위한 인증의 핵심요소로 각광받을 것으로 전망되고 e메일 보안은 콘텐츠 필터링, 암호화 서비스 등을 결합한 턴키 베이스 솔루션이 부각될 것으로 예상된다.

ESM은 시스템 하나로 다 각도의 보안관리를 할 수 있는 통합보안시스템이다. 통합보안시스템은 9가지의 보안관리가 이루어지고 특수 문 구축, 로비게이크 구축, 엘리베이터 통제, 방문객관리, IBS연동(전력, 공조, 소방), 위치 추적 시스템, 재실 관리 시스템, 순찰 관리 시스템, 외곽 보안 시스템이 바로 그것이다[[11].

2. 기업보안관리 시스템의 매출 현황

기업보안관리(ESM: Enterprise Security Management)는 방화벽, 침입방지시스템(IPS), 가상사설망(VPN) 등의 보안 솔루션을 하나로 모은 통합 보안관리시스템으로, 2008년도 매출액은 31,652백만원으로 2007년도 매출액은 30,219백만원에 비해 1,433백만원(4.5%) 증가하였다[8]. 연평균성장률 4.6%로 꾸준히 성장하여 2013년도 매출액은 39,627백만원 규모까지 증가할 것으로 추정된다. 최근 기업보안관리가 통합관리 수준을 넘어 기업자원관리시스템까지 확대·개발되고 있는 추세를 고려해보면 매출이 계속 증가할 것으로 예상된다. 아래의 [그림 2]는 ESM 매출 전망을 나타낸 그래프이다.

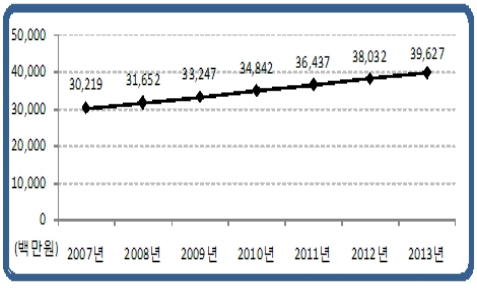

그림 2. ESM의 매출전망

기업보안관리(ESM)는 각 산업군별로 보안장비들을 어느 정도 갖춘 상태로 앞으로도 꾸준한 성장세를 기록할 것으로 보고 있다. 기존에 이미 구축되어진 공공·금융·일반 기업들의 업그레이드가 이미 시작됐고 지방자치단체 및 교육(대학, 교육청 등)권을 중심으로 새로운 수요처가 발생하고 있기 때문에 기업보안관리(ESM)의 매출은 꾸준하게 유지될 것으로 전망된다.

3. ESM 시장 및 기술 동향

보안관리가 진화하고 있다. 보안의 중요성이 강조되면서 도입된 수많은 보안 솔루션은 관리의 어려움을 증가시키고 있고, 각기 다른 장비가 쏟아내는 수많은 정보들로 효율적인 전사적 보안 체계 마련의 필요성이 대두되고 있기 때문이다.

국내에서는 ESM(Enterprise Security Management)이 보안관리를 대표했지만, 이를 더욱 고도화해야 한다는 요구가 증가하고 있는 것. 이에 RMS(Risk Management System), SIEM(Security & Event Management), TMS(Threat Management System) 등이 등장해 ESM을 보완하고, 전사적 관점에서의 보안 향상 방안을 마련하자는 움직임이 활성화되고 있다[8]. 특히 증가되는 보안 위협과 더불어 강화되는 IT 컴플라이언스는 SIEM, RMS 등 차세대 솔루션에 대한 관심을 더욱 높이고 있다.

3.1 통합 보안관리 솔루션

최근 통합 보안관리 아키텍처를 발표한 이글루시큐리티는 보안관리의 변화를 보여주는 사례라고 할 수 있다. 이글루시큐티가 발표한 통합 보안관리 아키텍처 '익스트림(eXTRiM)'은 국내 ESM의 최강자로 꼽히는 이글루시큐리티가 제시하는 차세대 보안 아키텍처로 관심을 모으고 있다[14].

이글루시큐리티는 통합 보안관리 아키텍처인 익스트림의 핵심은 복합형 종합 다차원 분석 시스템인 '스파이더시그마(SPiDER-∑)'다. 스파이더시그마는 ESM과 ESM(스파이더 TM)과 RMS(스파이더X)는 물론 침해 발생 시 대응과정을 프로세스화한 침해대응시스템(스파이더존) 등을 포괄해 위협상황과 더불어 대응상황, 위협의 위험 정도를 한꺼번에 시각적으로 보여줌으로써 보다 효과적인 정보보호를 구현하도록 한다.

3.2 데이터 수집의 통합

취약성 관리 프로그램의 효과는 단순히 사용되는 기술 뿐 아니라 구성요소 간 통합에 크게 좌우된다. 취약성 스캐너나 시스템 정책 및 장비 구성 감사툴 같은 취약성 식별 프로그램은 기본적인 데이터 수집 기능은 제공하지만 변화 관리 소프트웨어의 긴밀한 통합 또는 필요하다.

예를 들어 구성 관리, 패치 관리, 신원정보 및 액세스 관리 툴은 시스템의 유지보수를 자동화하고 시스템과 장비 상태에 대한 실시간 뷰를 제공하는데, 이런 제품에 취약성 식별 툴을 통합함으로써 기업에서는 취약성

과 위험에 대한 전체 그림을 얻을 수 있다. 하지만, 유지보수와 취약성 식별 시스템의 통합은 말처럼 쉬운 일이 아니에 대악쇠는 프로그램에 어떤 구성요소가 필수인지를 알아내는 것으로 보다 추천되는 방식은 하향식(top-down)이다.

IT 팀에서는 이에 대한 대답을 준비하면서 동시에 행동에 필요한 정보까지 수집해야 한다. '유럽 지역에 100개의 윈도우 시스템이 있다는 정보만으로 충분한가', 'MAC 어드레스를 알아야 하는가', '자산소유자는' 등의 대한 대답이 마련돼야만 추가 기술들을 고려할 수 있게 된다.

3.3 우선순위 지정

우선 지정은 IT에서 얼마나 언제나 매우 중요하지만, 특히 변화의 시기에는 그 중요도가 더더욱 증가된다. 분명 취약성 관리는 우선순위 지정에 수월한 방식으로 배치가 돼야 하는데, 이를 위해서는 보통 데이터 수집의 효과를 높일 수 있게 자산 그룹을 만들고, 관련성이 있고 행동으로 연결될 수 있는 보고를 만들기 쉽도록 소유자 그룹을 만드는 작업이 필요하다.

그룹은 지역적, 운영적(고객관리, 설비), 혹은 기술적 경계(데스크톱 그룹, 유닉스 팀)에 따라 만들어지는 경우가 많다. 따라서 보안 상태를 결정할 때는 자산 규모는 반드시 관리가 가능한 수준이어야 할 것이며, 책임도 명확히 규정돼야 할 것이다.

3.4 후속 작업

이후에도 계속돼야 할 작업은 개별적인 특성들이 취약성 관리 프로그램의 목표에 어떤 영향을 미치는지 파악하는 일이다. 아래의 [표 1]은 취약성 관리라는 목표 달성을 위한 사항에 힌트가 될 것이다. 보안 상태와 규정준수 레벨을 결정할 때는 양질의 데이터가 최고다. 놓친 취약성은 보안에 대해 그릇된 인식을 줄 수 있으며, 데이터가 잘못되면 '오탐지(false positive)', 즉 존재하지 않는 취약성을 만들어낼 가능성이 있다.

표 1. 목표달성에서 중요한 것들

특성	공격 면적 축소	보안 상태 파악	규정준수 달성
데이터 양	필수	선택	필수
데이터 품질	선택	필수	필수
높은 빈도	필수	선택	불필요
상호연관	필수	선택	불필요
동향추적	선택	필수	불필요
긍정-오류 줄이기	선택	불필요	필수
핵심 성능 지표	선택	필수	필수

공격 면적 축소가 최고 우선순위일 때는 데이터가 자주 수집돼야지만. 보안 상태를 결정할 때는 이것이 그리 중요하지 않다. 규정준수에서 데이터 수집 빈도의 중요성은 개인의 규정준수 필요조건에 따라 달라질 것이다.

동향 추적은 보안 상태와 취약성 축소 작업의 성공, 그리고 규정준수 관련 활동들을 파악하는 데 있어 가장 유용하다. 동향 정보에서는 시간이 경과하는 동안 조직의 위험 프로파일 변화와 취약성과 패치 발표 등과 같은 외부적인 사건들이 전사적인 보안 상태에 어떤 영향을 미치는지를 보여준다.

긍정 오류는 종종 존재하지 않는 취약성과 구성 에러를 보여준다. 동향 추적으로 이러한 긍정 오류를 줄일 수 있지만 이들은 여전히 규정준수 활동에 심각한 영향을 미칠 수 있다. 그 이유는 취약성이 정확한 그림이 규정 준수 보고에 매우 중요하기 때문이다.

4. 기업보안관리 시스템 적용 효과

4.1 비용측면

보안이 매우 중요하다는 것은 인정하지만, 당장의 우선순위에서 밀려나는 모습을 많이 보아왔다. 아직까지 IT예산에 보안 부문을 많이 배정하고 있지 않은 이유는 고가의 보안제품을 도입한다고 해도 순식간에 눈에 보이는 투자효과를 보여주지는 않기 때문이다. 이로 인해 CEO나 경영진들은 보안예산 투자를 꺼리게 된다.

4.2 관리의 효율성

ESM의 의의는 관리의 효율성 차원에서 살펴 볼 수 있다. 가트너 그룹이 조사한 TCO(Total Cost of

Ownership) 모델에 따르면 기업 IT 비용의 2/3에서 3/4정도가 인력을 배치하고 관리하며 유지하는 등의 비용으로 지출된다고 한다. ESM은 이처럼 수많은 관리자가 해야 할 반복적이고 단순한 업무들을 자동화하고 단순화함으로써 전체적인 비용 절감 효과를 가져 올 수 있다. 또한 분산되어 있는 기업 IT 환경에서 전사적인 차원의 관리가 가능하기 때문에 일관되고 효율적인 보안 관리를 가능케 한다.

Ⅲ. ESM 보안성 품질요구사항

이 절에서는 기업보안관리 시스템의 품질 요구사항에 관련해서 고유한 특성인 보안성과 보안성능에 관한 요구사항을 분석하여 지식정보보안 제품의 품질평가 기준 및 방법론을 구축하기 위한 기반을 확립하고자 한다.

다시 말해, 기업보안관리 시스템의 고유 품질 요구사항은 보안성과 효율성의 부특성인 보안성능을 중심으로 구성되며, 지식정보보안 제품의 특성에 따라 공통적인 품질 요구사항과 차별적인 품질 요구사항으로 구분된다[7]. 다음의 [표 2]는 ESM 제품의 요구사항에 따른 보안성에 관한 평가 항목과 효율성의 성능에 관한 평가 항목의 관련성을 나타낸 것이다.

표 2. ESM의 보안성 및 효율성 품질 요구사항

특성	부특성	평가 항목명	ESM
보안성	보안 감사	보안 경보	○
		감사 데이터 생성	○
		감사 데이터 수집	○
		사건과 사용자 연관	○
		감사 검토	○
		감사 검토 권한 제한	
		저장소 보호	○
		대응 행동	○
		손실 방지	○
	사용자 데이터 보호	정보흐름 통제	
		부분적인 접근통제	○
		보안 속성에 따른 통제	○
		보안속성 없는 사용자 데이터 접근통제	○
		내부전송 보호	○
		잔여정보 보호	
		무결성 검사 및 대응행동	
	식별 및 인증	인증 실패 처리	○
		사용자 보안속성 유지	○
		사용자 인증	
		인증 피드백 보호	
		재사용 방지	
		사용자 식별	○
	보안 관리성	보안기능 관리	○
		보안속성 관리	○
		보안속성 폐지 권한	
		한계치 관리 제한	
		관리기능 수행	○
		관리자 역할 유지	
		보안 역할 유지	○
		안전한 상태 유지	○
	보안 기능 보호	재사용 탐지	
		재사용 대응	
		자체 시험	○
효율성	보안 성능	최대 패킷 처리량	○
		터널 처리량	
		초당 연결수	○
		초당 트랜잭션 수	○
		전송지연	○
		최대 누적 HTTP 연결수 처리량	
		최대 세션 처리량	○
		최대 세션수	○
		동시세션 유지율	
		초당 TCP 처리성능	
		공격 차단 성능	○

Ⅳ. 기업보안관리 보안성 평가방법 기준

본 연구에서는 분류체계 소프트웨어 제품평가에 관한 국제표준인 ISO/IEC9126에서 기능성의 부특성이었던 보안성을 별도의 품질특성으로 도출한 것이다. 이는 기업보안관리 제품의 특성을 고려하여 ISO/IEC 25000 시리즈의 표준화 동향을 반영한 것이다[1-3].

1. 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 소프트웨어의 능력을 의미한다. 보안성은 보안감사성, 사용자 데이터 보호, 식별 및 인증, 보안관리성, 보안기능 보호, 접근통제성, 준수성 등의 평가항목을 가진다.

1.1 보안감사성

보안감사성이란 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 의미한다. 보안감사성은 보안 경보, 감사 데이터 수집, 감사 데이터 생성, 사건과 사용자 연관, 규칙위반 지적, 복잡공격 학습, 감사 검토, 저장소 보호, 대응 행동, 손실 방지의 평가항목을 가진다.

다음의 [표 3]은 보안성 부특성인 보안감사성의 평가항목을 나타낸 것이다.

표 3. 보안감사성 평가항목

번호	특성	부특성	평가 항목명	평가항목의 목적
1	보안성	보안 감사성	보안 경보	보안위반 탐지시 대응행동의 목록을 취하는가를 평가
2	보안성	보안 감사성	감사 데이터 수집	관리대상 시스템이 생성하는 감사 데이터 정보를 수집할 수 있는 기능을 제공하는가를 평가
3	보안성	보안 감사성	감사 데이터 생성	규정된 감사데이터를 생성하는지 평가
4	보안성	보안 감사성	사건과 사용자 연관	사건을 발생시킨 사용자의 신원과 감사 대상 사건을 연관시킬 수 있는지 평가
5	보안성	보안 감사성	규칙 위반 지적	사건을 검사시, 규칙집합을 적용하고 규칙에 기반하여 잠재적 위반을 지적할 수 있는지 평가
6	보안성	보안 감사성	감사 검토	감사레코드로부터 모든 감사데이터를 제공하는지를 평가
7	보안성	보안 감사성	저장소 보호	인가되지 않은 삭제로부터 감사 레코드를 보호하는지 평가
8	보안성	보안 감사성	대응 행동	감사 데이터가 한도를 초과할 경우, 관리자에게 통보하고 대응행동을 취하는지 평가
9	보안성	보안 감사성	손실 방지	감사 증적이 포화인 경우, 감사 저장 실패시 취해야 할 행동을 수행하는지 평가

1.2 사용자 데이터 보호

사용자 데이터 보호란 지식정보보안 제품 장애 발생시 안전한 상태를 유지하고 보안 관련 데이터 및 실행 코드의 무결성을 검증하기 위하여 자체 시험을 수행하며 사용자 비활 기간 이후에 대한 세션 관리 기능을 제공하는 능력을 의미한다. 사용자 데이터 보호는 부분적인 접근통제, 보안속성에 따른 통제, 보안속성 없는 사용자 데이터 접근통제, 내부전송 보호의 평가항목을 가진다. [표 4]는 사용자 데이터 보호 평가항목을 나타낸 것이다.

표 4. 사용자 데이터 보호 평가항목

번호	특성	부특성	평가 항목명	평가항목의 목적
1	보안성	사용자 데이터 보호	부분적인 접근통제	보안기능이 주체와 객체 간의 오퍼레이션에 대해 접근통제를 수행하는지 평가
2	보안성	사용자 데이터 보호	보안 속성에 따른 통제	보안속성에 따라 정보흐름을 통제하는지 평가
3	보안성	사용자 데이터 보호	보안속성 없는 사용자 데이터 접근통제	외부에서 유입되는 사용자 데이터에 대해 접근통제를 강제하는지 평가
4	보안성	사용자 데이터 보호	내부전송 보호	사용자 데이터가 물리적으로 분리된 대상 간에 전송될 때 노출, 변경을 방지하기 위해 접근통제를 강제하는지 평가

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. 식별 및 인증은 인증실패 처리, 사용자 보안속성 유지, 비밀정보 검증, 관리자 인증, 관리자 식별, 사용자 식별의 평가항목을 가진다. 다음의 [표 5]는 식별 및 인증 평가항목을 나타낸 것이다.

표 5. 식별 및 인증 평가항목

번호	특성	부특성	평가 항목명	평가항목의 목적
1	보안성	식별 및 인증	인증 실패 처리	인증 실패를 탐지하고 대응행동을 수행하는지를 평가
2	보안성	식별 및 인증	사용자 보안속성 유지	각 사용자에 대해 규정된 보안속성 목록을 유지하는지 평가
3	보안성	식별 및 인증	비밀정보 검증	비밀정보가 허용기준을 만족시킴을 검증하는 메커니즘을 제공하는지 평가
4	보안성	식별 및 인증	관리자 인증	명시된 행동 이외의 다른 모든 행동을 허용하기 전에 관리자를 성공적으로 인증하는지 평가
5	보안성	식별 및 인증	관리자 식별	명시된 행동 이외의 다른 모든 행동을 허용하기 전에 관리자를 성공적으로 식별하는지 평가
6	보안성	식별 및 인증	사용자 식별	사용자에게 행동을 허용하기 전에 각 사용자를 성공적으로 식별하는지 평가

1.4 보안관리성

보안관리성이란 해당 지식정보보안 제품의 보안기능,

보안속성, 보안 관련 데이터, 보안 역할 등과 관련된 사항을 관리하는 능력을 의미한다. 보안관리성은 보안기능 관리, 보안속성 관리, 디폴트 값 제공, 데이터 관리 제한, 관리기능 수행, 보안역할 유지의 평가항목을 가진다. [표 6]은 보안관리성 평가항목을 나타낸 것이다.

표 6. 보안관리성 평가항목

번호	특성	부특성	평가 항목명	평가항목의 목적
1	보안성	보안 관리성	보안기능 관리	인가된 관리자만 보안기능을 관리할 수 있도록 제한하는지 평가
2	보안성	보안 관리성	보안속성 관리	보안속성을 인가된 관리자만 다룰 수 있도록 제한하는지 평가
3	보안성	보안 관리성	디폴트 값 제공	보안속성의 디폴트값을 제공하도록 강제하는지 평가
4	보안성	보안 관리성	데이터 관리 제한	식별 및 인증 데이터의 관리를 인가된 관리자로 제한하는지 평가
5	보안성	보안 관리성	관리기능 수행	규정된 관리 기능을 수행하는지 평가
6	보안성	보안 관리성	보안역할 유지	보안기능이 인가된 역할을 유지하는지 평가

1.5 보안기능 보호

보안기능 보호란 보안기능을 주기적 또는 관리자의 요구에 따라 무결성을 검증하는 능력을 의미한다. 보호는 안전한 상태 유지, 자체 시험의 평가항목을 가진다. [표 7]은 보안기능 보호 평가항목을 나타낸 것이다.

표 7. 보안기능 보호 평가항목

번호	특성	부특성	평가 항목명	평가항목의 목적
1	보안성	보안기능 보호	안전한 상태 유지	장애 발생시에도 안전한 상태를 유지하는지 평가
2	보안성	보안기능 보호	자체 시험	데이터 및 실행코드의 무결성을 검증하기 위해 자체 시험을 실행할 수 있는가를 평가

2. 보안성 품질 검사표

기업정보보안 제품의 보안성 측정 항목을 구체적으로 도출하기 위한 방법으로서 점검표를 정리하였다. 점검표의 세부항목을 체크한 결과를 집계합으로써 측정항목의 결과가 도출될 수 있다. [표 8]은 앞에서 보였던 부특성의 평가항목의 품질 검사표에 대해서 나타낸 것이다.

표 8. 보안성 품질 검사표

번호	평가메트릭		내 용
1	감사 데이터 생성	측정항목A	생성하도록 규정된 감사데이터의 수
		측정항목B	생성된 감사데이터의 수
		측정식	보안 경보 = B/A
		측정 영역	0 ≤ 감사데이터 생성 ≤ 1
2	정보흐름 토제	측정항목A	정보흐름에 관련된 모든 기능의 수
		측정항목B	정보흐름이 통제되는 기능의 수
		측정식	인증실패 처리 = B/A
		측정 영역	0 ≤ 정보흐름 통제 ≤ 1
3	관리자 인증	측정항목A	관리자 인증 후에 행동이 허용되는지의 여부
		측정식	관리자 인증 = A
		측정 영역	관리자 인증 = Yes or No
4	보안기능 관리	측정항목A	비인가자의 보안관리 접근 차단 여부
			- 보안기능 : 보안정책 수행에 기여하는 모든 하드웨어, 소프트웨어, 펌웨어로 구성된 집합
		측정식	보안기능 관리 = A
		측정 영역	보안기능 관리 = Yes or No
5	안전한 상태 유지	측정항목A	장애 발생 수
		측정항목B	전한 상태를 유지하는 경우의 수
		측정식	안전한 상태 유지 = B/A
		측정 영역	0 ≤ 안전한 상태 유지 ≤ 1
6	보안성 표준 준수율	측정항목A	평가할 보안성 표준 준수 항목 수
			- (다음과 같은 유형의 정보 제공 여부를 파악) - 보안성 표준 준수와 관련된 정보 - 제품이 준수하는 보안성 관련 규정, 기준 및 사용지침
		측정항목B	각 항목별 테스트케이스 성공률의 합
			-테스트케이스를 시험하여 성공한 경우를 체크
		측정식	- 보안성 표준 준수율 = B/A - B = $\sum_{i=1}^{A} \frac{Success\_TC_i}{Total\_TC_i}$ - Success_TC : i 번째 기능 확인을 위해 수행한 테스트케이스 중 성공한 건 수 - Total_TC : i 번째 기능 확인을 위해 수행한 테스트케이스 수
		측정 영역	0 ≤ 보안성 표준 준수율 ≤ 1

V. 품질 측정과 성능 시험 평가

본 평가 사례에서는 기업내에 관리 대상 클라이언트에 설치된 안티 바이러스 프로그램을 업데이트 및 관리하는 안티 바이러스 통합 관리 프로그램으로 기능은 접근제어 설정, 보조서버 설정, DB 설정, 로그관리, 관리자 설정, 사이트 관리, 정책 적용, 실시간 감지기 제어 등의 기능을 갖춘 프로그램에 대해서 측정하였다. 그리고 평가한 사례에서 보안성에 관한 평가 사례를 통해 평가 방법에 대해 소개 하겠다.

1. 시험 환경

소프트웨어를 평가하기 위한 시험 환경 구축에 대해 기술 하였다.

(1)번 서버에 설치한 프로그램은 시험 대상 제품(서버 콘듈, 콘솔 모듈)과 DBMS: Microsoft SQL Server 2005을 설치하였으며 (2)번 보조서버에도 마찬가지로 시험 대상 제품(서버 콘듈, 콘솔 모듈)을 설치하였다. 그리고 클라이언트 (3)~(6)번엔 시험대상 제품인 에이전트 모듈을 설치하였다. 그리고 (1)번 서버와 (3)~(6)번 클라이언트엔 Performance Logs and Alerts(자원사용률 측정)을 설치하였다.

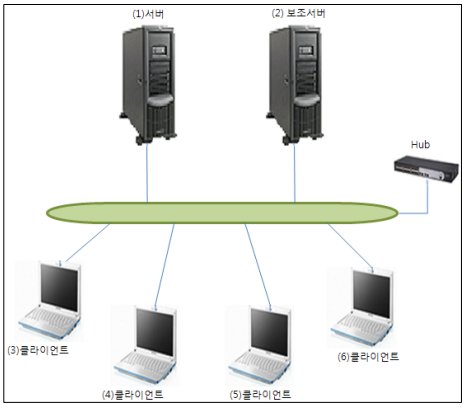

그림 3. 시험환경

2. 효율성 시험 결과

CPU 사용률은 서버 서비스를 구동시키는 경우, 서버의 CPU 사용률은 42.97%까지 올라갔지만 처리완료 후 1% 미만으로 유지가 되며, 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 유지된다.

서버에서 다수의 클라이언트로부터 1,000개, 2,000개의 바이러스 이벤트 로그를 수집하는 경우, 서버의 CPU 사용률은 각각 30.86%, 54.30%까지 올라갔지만 처리완료 후 모두 1% 미만으로 유지된다.

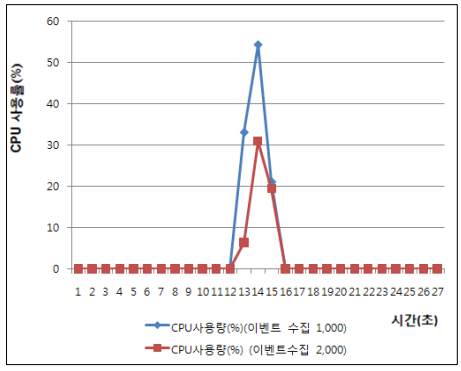

그림 4. (1)번 서버 CPU 사용량

메모리 사용량은 서버 서비스를 구동시키는 경우, 서버의 메모리 사용량은 541~550MB로 일정하게 유지되며, 에이전트 서비스를 구동시키는 경우, 클라이언트의 메모리 사용량은 (3), (4), (5), (6)번 클라이언트에서 각각 280~285MB, 391~397MB, 384~389MB, 391~395MB로 일정하게 유지된다.

서버에서 다수의 클라이언트로부터 1,000개, 2,000개의 바이러스 이벤트 로그를 수집하는 경우, 서버의 메모리 사용량은 각각 583~584MB, 578~580MB로 일정하게 유지된다.

3. 보안성 품질 측정

[표 9]는 품질부특성에 대한 집계 결과를 나타낸 것으로 품질부특성의 집계는 [표 9]의 메트릭 결과로부터 각 부특성에 대한 메트릭값의 합계를 평균한 것이다. 결과를 통해 각 품질특성별로 취약한 결과를 보이고 있는 부특성들을 확인할 수 있다. 선정은 평가 대상 소프

트웨어의 특성을 고려하여 중요성이 낮거나 평가 대상이 준비되어 있지 않거나 적용하기에 적합하지 않은 것들은 제외될 수 있다.

메트릭 결과에 대해 메트릭 측정값의 범위에 따라 매우미흡(0.6미만), 미흡(0.6이상-0.7미만), 보통(0.7이상-0.8미만, 우수(0.8이상-0.9미만), 매우우수(0.9이상) 등으로 레벨을 분류할 수 있으나 축적된 평가결과를 분석하는 연구를 통해 타당성이 검증될 필요가 있다.

표 9. 보안성 품질 측정표

품질특성	부특성	평가 항목	측정값	비고
보안성	보안감사성	보안경보	0.97	
		감사데이터 수집	0.92	
		사건과 사용자 연관	0.89	
		규칙위반 지적	1.00	
		대응 행동	1.00	
		손실방지	0.97	
	사용자 데이터 보호	부분적인 접근통제	0.95	
		보안속성에 따른 통제	0.88	
		내부전송 보호	1.00	
	식별 및 인증	인증 실패 처리	1.00	
		사용자 보안속성 유지	0.96	
		비밀정보 검증	0.82	
		관리자 인증	1.00	
		관리자 식별	1.00	
	보안 관리성	보안기능 관리	0.92	
		보안속성 관리	0.84	
		데이터 관리 제한	0.85	
		보안 역할 유지	0.91	
	보안기능 보호	안전한 상태 유지	1.00	
		자체 시험	0.92	
평 균			0.94	

보안성에 관련해서 평균 0.94로 전반적으로 우수한 결과를 나타내고 있음을 알 수 있다.

Ⅵ. 결 론

기업보안관리 시스템 제품은 양적으로는 빠른 성장세를 보이고 있으나 그 동안 질적인 품질을 고려하는 노력이 미흡한 것이 사실이었다. 따라서 본 논문에서는 기업보안관리 시스템 제품의 질적인 면을 평가하여 품질수준을 파악하여 개선방향을 도출함으로써 품질향상을 지원할 수 있는 평가모델을 개발하기 위해 제품의 동향 및 기술적인 요소들을 조사 분석하였다.

또한 기업보안관리 시스템 제품의 특성을 고려하고 제품의 고유한 품질 요구사항을 도출한 필요가 있는 요소를 분류하여 분석함으로써 기업보안관리 시스템 보안성 평가 모델 및 방법론을 개발하였다.

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

그리고 제품의 보안성 품질을 측정하고 그 결과를 적절한 기준에 따라 판정하는 방법에 대해 연구를 수행하고자 성능시험사례를 제시하여 평가방법을 제시하였다.

향후 연구에서는 기업보안관리 시스템 제품에 대한 지속적인 시험평가를 통해 사례를 축적함으로써 평가방법론의 타당성을 제고하는 검증 연구를 수행해야 할 것이다.

참 고 문 헌

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

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

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

[4] International Data Corporation(IDC), "Worldwide Security Appliance Forecast and Analysis 2003-2007, 2003.

[5] Bat-Erdene Munkhbayar, Esbold Unurkhaan and Tsogtsalkhan Anar and Damdinsuren Erdenechineg, "Network Security Mangement in MUST", ICEIC 2006, pp.227-230, 2006(1).

[6] S. E. Coull, M. P. Collins, C. V. Wright, F. Monrose, and M. K.Reiter, "On Web Browsing Privacy in Anonymized NetFlows," 16Tth USENIX Security Symposium, 2007(8).

[7] 한국인터넷 진흥원, "국내 정보보호산업 시장 및 동향 조사", 2007.

[8] 이대식, 윤동식, 안희악, "ESM 시스템을 이용한 안정된 학내망 구축", 정보보증논문지, 제5권, 제3호, 2005(9).

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

[10] 김동진, "기업환경의 내부보안을 위한 통합 보안 관리 시스템의 설계 및 구현", 창원대학교, 2008.

[11] 한국정보통신기술협회, "소프트웨어 테스트 전문기술", 기초과정편, TTA, 소프트웨어시험인증센터, 2006.

[12] 한국정보통신기술협회, "소프트웨어 테스트 전문기술", 응용과정편, TTA, 소프트웨어시험인증센터, 2006.

[13] 최대수, 이용균, "ESM에서 보안이벤트 분석 기술에 관한 연구", 한국정보과학회, 학술발표논문집, 제4권, 제1호(D), 2007(6).

[14] 김석훈, 김은수, 송정길, "통합 보안 관리 시스템에서의 침입탐지 및 대응을 위한 보안 정책 모델에 관한 연구", 정보보증논문지, 제5권, 제2호, 2005(6).

저 자 소 개

차 영 환(Young-Hwan Cha) 정회원

- 1981년 2월 : 서울대학교 사범대학 과학교육과 졸업(학사)
- 1988년 2월 : 연세대학교 전자계산학과 졸업(석사)
- 2006년 6월 : KAIST 최고경영자 과정 수료
- 2009년 8월 : 서울벤처정보대학원대학교 컴퓨터응용기술학과 박사과정 수료
- 1981년 2월 : 한국산업은행 입행
- 2008년 2월 ~ 현재 : 한국산업은행 원주 지점장

<관심분야> : 전자계산관련분야, 소프트웨어공학(SW 품질보증과 품질평가)

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