기업보안관리(ESM) 제품의 평가모델 개발

강상원*, 전인오**, 양해술**
*호서대학교 혁신기술경영융합대학원
**호서대학교 벤처전문대학원
e-mail:myksangwon@paran.com, hsyang@office.hoseo.ac.kr

Development of Evaluate Model of Enterprise Security Management (ESM) Product

Sang-Won Kang*, In-Oh Jeon**, Hae-Sool Ynag*
*Graduate School of Multidisciplinary Technology and Management, Hoseo Univ
**Graduate School of Venture, Hoseo Univ

요 약

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 있다. 본 연구에서는 기업보안관리(ESM) 제품의 질적인 면을 평가하고 품질수준을 파악하여 개선방향을 도출함으로써 품질향상을 지원할 수 있는 보안성 평가모델과 시험 방법론에 대해서 개발하였다.

1. 서론

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 일반화된 현재는 열린 환경 속에서 개인적인 정보 자산을 지키기는 일이 무엇보다 중요하다는 것이다.

정보보호 시장은 단순 보안제품의 구매/설치의 시장에서 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 보안 제품에 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. 이러한 니즈에 맞추어, 기업보안관리(Enterprise Security Management, 이하 ESM)를 위한 통합보안관제시스템 또는 이러한 시스템을 도구로 이용하는 보안 관제 서비스가 등장하게 되었다.

† 본 연구는 지식경제부와 정보통신연구진흥원의 대학IT연구센터 지원사업의 연구결과로 수행되었음(NIPA-2010-(C1090-1031-0001))

2. 기업보안관리 시스템의 기술 유형

2.1 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 잇도록 데이터를 관리한다.

2.2 재실 관리 시스템

입구, 출구에 각각의 보안단말기를 설치하여 각

층 및 각 사무실의 정확한 인원파악이 가능하다. 안전 문제 발생시 현장의 정확한 인원파악으로 신속한 대응이 가능하다.

2.3 순찰 관리 시스템

순찰계획에 따라 순찰자의 시간 및 위치를 상시 감시하며 체계적이고 효율적인 순찰관리가 가능하다. 순찰자와 외부인에 대한 통제를 한번에 관리할 수 있다.

2.4 외곽보안시스템

기업정보(연구자료, 영업 활동 등)유출을 방지하기 위한 시스템이다. CCTV와 연계 운영하면 정보 유출자도 추적이 가능하고 티스켓이 유출 됐을 경우에도 추적할 수 있다.

3. 시스템 적용 효과

3.1 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.

3.2 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.

4. 기업보안시스템 평가방법 기준

4.1 기능성 평가항목

기능성이란 소프트웨어가 특정 조건에서 사용될 때, 명시된 요구와 내재된 요구를 만족하는 기능을 제공하는 소프트웨어 제품의 능력을 의미한다. 기능성은 적합성, 정확성, 상호운영성, 준수성 등의 품질 부특성으로 세분화 된다.

[표 1] 기능성 평가항목

부특성	평가 항목명	평가항목의 목적
적합성	기능 구현 완전성	문서에 기술되어 있는 기능의 구현 여부
	기능 충분성	기업정보보안시스템에 필요한 필수적인 기능이 충분히 구현되어 있는지 여부
	기능 적절성	평가된 각 기능이 기업정보보안시스템을 구성하는 기능 요소로서 적절한지 여부를 평가
정확성	기능 구현 정확성	기업정보보안시스템의 각 기능이 명세된 대로 구현되어 요구하는 수준에 부합하는지 여부를 평가
	정밀성	제품의 결과 값이 사용자 문서에 기술되어 있는 결과값의 정밀도와 동일하게 구현되어 있는지 여부
정확성	기능 구현 정확성	기업정보보안시스템의 각 기능이 명세된 대로 구현되어 요구하는 수준에 부합하는지 여부를 평가
준수성	기능표준 준수율	기업정보보안 시스템의 기능 관련 표준이나 규약에 따라 동작하는지 평가

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

[표 2] 보안성 평가항목

부특성	평가 항목명	평가항목의 목적
보안감사성	보안 경보	보안위반 탐지시 대응행동의 목록을 취하는가를 평가
	감사 데이터 수집	관리대상 시스템이 생성하는 감사 데이터 정보를 수집할 수 있는 기능을 제공하는가를 평가
	감사 데이터 생성	규정된 감사데이터를 생성하는지 평가
	사건과 사용자 연관	사건을 발생시킨 사용자의 신원과 감사대상 사건을 연관시킬 수 있는지 평가
	규칙 위반 지적	사건을 검사시, 규칙집합을 적용하고 규칙에 기반하여 잠재적 위반을 지적할 수 있는지 평가

	복잡공격 학습	시스템 행동이 잠재적 위반임을 나타내는 시그너처 사건이나 연속된 사건과 일치할 때, 보안기능이 잠재적인 위반임을 지적할 수 있는지 평가
	감사 검토	감사레코드로부터 모든 감사데이터를 제공하는지를 평가
사용자 데이터 보호	부분적인 접근통제	보안기능이 주체와 객체 간의 오퍼레이션에 대해 접근통제를 수행하는지 평가
	보안 속성에 따른 통제	보안속성에 따라 정보흐름을 통제하는지 평가
	보안속성 없는 사용자 데이터 접근통제	외부에서 유입되는 사용자 데이터에 대해 접근통제를 강제하는지 평가
	내부전송 보호	사용자 데이터가 물리적으로 분리된 대상 간에 전송될 때 노출, 변경을 방지하기 위해 접근통제를 강제하는지 평가
보안 관리성	보안기능 관리	인가된 관리자만 보안기능을 관리할 수 있도록 제한하는지 평가
	보안속성 관리	보안속성을 인가된 관리자만 다룰 수 있도록 제한하는지 평가
	디폴트 값 제공	보안속성의 디폴트값을 제공하도록 강제하는지 평가
	데이터 관리 제한	식별 및 인증 데이터의 관리를 인가된 관리자로 제한하는지 평가
	관리기능 수행	규정된 관리 기능을 수행하는지 평가
	보안역할 유지	보안기능이 인가된 역할을 유지하는지 평가

4.3 신뢰성 평가항목

신뢰성이란 명세된 조건에서 사용될 때, 성능 수준을 유지할 수 있는 소프트웨어의 능력을 의미한다. 신뢰성은 성숙성, 결함 허용성, 회복성, 준수성 등의 품질 부특성으로 세분화 된다.

[표 3] 신뢰성 평가항목

부특성	평가 항목명	평가항목의 목적
성숙성	문제 해결률	이전 버전의 기업정보보안시스템에 존재하던 문제에 대하여 명시적으로 해결이 확인되는 정도를 평가
	결함 회피율	일정한 운용 시간 내에 결함이 발생하지 않는 정도를 평가
	결함발생 평균시간	기업정보보안 시스템의 결함발생 평균시간(MTBF)를 평가
결함 허용성	다운 회피율	발생되는 결함 중 시스템 다운을 가져오는 결함이 발생하지 않는 정도
결함 허용성	장애 회피율	발생되는 결함 중 장애를 발생시키는 정도의 심각한 결함이 발생하지 않는 정도
회복성	데이터 복구율	결함이 발생할 경우에 데이터가 복구되는 정도
	이용 가능률	일정 시간 사용중에 시스템이 다운이나 기타 이유로 인하여 사용할 수 없는 기간을 평가
	평균 복구 시간	시스템에 결함이 발생되었을 경우 복구가 시작되어 완료되기까지 소요되는 복구 평균 시간을 평가
준수성	신뢰성 표준 준수율	기업정보보안 시스템의 신뢰성 표준에 따라 시스템이 구현되어 있는지 평가

4.4 사용성 평가항목

사용성이란 명시된 조건에서 사용할 경우 사용자가 이해하고, 학습하고, 사용하며 선호할 수 있는 소프트웨어의 능력을 의미한다. 사용성에는 이해가능성, 학습 가능성, 운영성, 선호도, 준수성 등의 품질 부특성으로 세분화 된다.

[표 4] 사용성 평가항목

부특성	평가 항목명	평가항목의 목적
이해 가능성	기능 이해도	제품 설명서와 사용자 문서를 읽고 제품이 제공하는 기능을 이해할 수 있는 정도를 평가
	인터 페이스 이해도	제품의 메뉴 및 기타 인터페이스를 보고 기능을 이해 할 수 있는 정도
	도움말 이해도	제품에서 제공하는 도움말(데모/튜토리얼)을 쉽게 이해할 수 있는 정도
	입출력 데이터 이해도	제품의 입력 및 출력에 사용되는 데이터를 쉽게 이해할 수 있는 정도
	인터페이스 일관성	인터페이스 요소들 간에 일관성 있게 구현된 정도
	사용자 안내성	제품이 사용자 수준에 따라 사용할 수 있게 하는 기능을 제공 하고 있는 정도
	메시지 이해 용이성	제품 사용시 나타나는 메시지의 이해 용이 정도
학습 가능성	기능 학습 용이성	사용자가 제품을 사용하기 위한 기능을 쉽게 학습할 수 있는 정도
	도움말 접근용 이성	사용자가 도움말을 쉽게 참조할 수 있는 정도
운영성	운영절차 일관성	제품 운영 절차가 균일하게 구조화 되어 있는 정도
	진행상태 파악 가능성	제품 진행 상태를 사용자에게 보여주는 기능 제공 정도
	오류 복구 용이성	제품을 사용하는 도중 발생한 오류를 쉽게 복구할 수 있는 방안 제공 정도
	문제해결 정보 제공	제품을 사용시 발생 문제해결을 위한 정보를 충분히 제공하고 있는 정도
선호도	인터 페이스 변경	사용자의 필요에 따라 제품의 인터페이스를 조정하는 기능이 있는 정도

	가능성	
선호도	인터페이스 선호도	인터페이스가 시각적으로 사용자에게 호감을 주는지 정도
준수성	사용성 표준 준수율	기업정보보안 시스템이 사용성과 관련된 표준, 규약에 따라 구현되었는지 평가

4.5 효율성 평가항목

효율성이란 명시된 조건에서 사용되는 자원의 양에 따라 요구된 성능을 제공하는 소프트웨어의 능력을 의미한다. 효율성에는 시간 효율성, 자원 효율성, 준수성 등의 품질 부특성으로 세분화 된다.

[표 5] 효율성 평가항목

부특성	평가 항목명	평가항목의 목적
시간 효율성	평균반응 시간의 적절성	제품 사용시의 사용자의 입력에 대한 평균반응 시간을 측정
	평균 처리율	제품에 주어진 시간내에 성공적으로 작업을 수행할 수 있는 평균 처리량을 측정
	평균처리 시간의 적절성	제품 사용중 특정한 업무를 성공적으로 수행하는 평균 처리 시간
자원 효율성	입출력 자원 사용률	기업정보보안시스템의 I/O자원의 사용 정도
	메모리 사용률	기업정보보안시스템의 메모리 사용 정도
	데이터 전송률	기업정보보안시스템의 데이터 전송 속도
	CPU 사용률	기업정보보안시스템의 CPU 사용 정도
성능	CPS (Connection Per Second)	초당 연결수가 적정 수준인가를 측정
	TPS (Transaction Per Second)	초당 트랜잭션의 수가 적정 수준인가를 측정
	Concurrent Session	제품이 처리할 수 있는 최대세션 수를 검증

5. 결 론

소프트웨어의 품질은 그 소프트웨어를 활용하는 업무의 품질을 근본적으로 좌우하는 중요한 요소이다. 소프트웨어 품질평가에 관한 국제표준이 제정된 이후, 국제표준을 다양한 소프트웨어 분야에 적용하기 위한 연구가 수행되어 왔으며 국내에서도 이러한 노력이 패키지 소프트웨어를 위시한 다양한 소프트웨어 분야의 시험인증 제도화 및 정착을 통해 가시화되었다.

본 연구에서는 기업보안관리 시스템 제품의 질적인 면을 평가하여 품질수준을 파악하여 개선방향을 도출함으로써 품질향상을 지원할 수 있는 평가모델을 개발하기 위해 제품의 동향 및 기술적인 요소들을 조사 분석하였다.

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

참고문헌

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

[4] Bat-Erdene Munkhbayar, Esbold Unurkhaan, Tsogtsalkhan Anar, Damdinsuren Erdenechineg, ″Network Security Mangement in MUST″, ICEIC 2006, pp.227~230, 2006. 1.

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

[6] 김동진, “기업환경의 내부보안을 위한 통합 보안관리 시스템의 설계 및 구현”, 창원대학교, 2008.

[7] 한국정보통신기술협회, “소프트웨어 테스트 전문기술”, 기초과정편, TTA, 소프트웨어시험인증센터, 2006.

[8] 한국정보통신기술협회, “소프트웨어 테스트 전문기술”, 응용과정편, TTA, 소프트웨어시험인증센터, 2006.

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