정보보안 소프트웨어 유지보수 요율 체계에 대한 연구

최명길*, 박은주**,
*중앙대학교 사회과학대학
**중앙대학교 경영대학
*e-mail : mgchoi@cau,ac,kr
**e-mail : ejlm2000@hanmail.net

A study on the Information security software for the rate of maintenance

Myeong-Gil Choi*, Eun-Ju -Park**
*College of Social Sciences, Chung-Ang University
**College of Business Adminstration, Chung-Ang University

요 약

정보화 사업의 확대와 함께 정보보안에 대한 사회적 관심은 보다 높아지고 있으며, 사이버 보안강화는 국가 및 기업의 인프라를 보호하기 위해 매우 중요한 부분이다. 그러나 정보보안 SW 유지보수 규모나 정보보안 SW의 특성과는 관계없이 유지보수 비용이 책정되어서 고품질의 유지보수 서비스를 기대하기 어려운 실정이다. 그러므로 정보보안 SW 유지보수의 규모와 유지보수 생산성에 영향을 미치는 제반요소를 발견하고, 이들을 비용에 연결시키는 정보보안 SW 유지보수 대가기준 마련이 필요하다. 이에 본 연구는 정보보안SW 유지보수의 특수성에 대한 분석을 통하여 보안업데이트, 모니터링·로그분석 및 정책 지원 등 추가적인 서비스 지원 등에 대한 유지보수 비용을 산정하고 일반 SW와의 원가비교 분석 조사를 통한 적정유지보수 요율을 도출하고자 한다. 또한, 정보보안 SW 유지보수 대가 구조분석 및 해외 사례 수집 분석, 설문조사, 전문가검증, 시뮬레이션 등을 통하여 정보보안 SW의 유지보수 대가 산정에 대한 기준의 도출이 필요하다. 이는 정보보안 SW의 유지보수 대가를 명확하게 산정하고, 사용자 및 공급자에게 적정한 대가 지급 기준을 수립함으로써 더 나아가 정보보안 SW 기업의 경쟁력 향상을 도모하고자 한다.

1. 서론

정보화 사업의 확대와 함께 정보보안에 대한 사회적 관심은 보다 높아지고 있으며, 사이버 보안강화는 국가 및 기업의 인프라를 보호하기 위해 매우 중요한 부분이다. 지속적인 정보보안에 대한 관심은 국가 및 기업의 정보체계 및 인프라 보호를 위한 투자로 이어지고 있으며, 전체 S/W의 유지보수 서비스 문제가 사회적으로 나타나고 있다.

전 세계 S/W의 유지보수 시장은 라이센스 중심의 사업 방식에서 유지보수 서비스 중심으로의 서비스 방향이 전환되는 현실에 비추어볼 때, 유지보수 서비스 시장은 지속적으로 성장할 것으로 사료된다.

현행 정보보안 SW 사업대가기준에서 유지보수 대가는 일반 SW 유지보수와 마찬가지로 변경/유지보수 규모실적, 정보보안 SW 특성과 무관하게 유지보수 시점에서의 SW 개발비용의 10~15% 범위 내에서 후발주자 간의 상호간의 협의에 의해 설정하도록 되어 있으나. '상호협의'라는 부분이 공공부문의 무상유지보수요구를 정당화하는 독소조항으로 악용될 수 있다.

특히 정보보안 SW 유지보수 규모나 정보보안 SW 특성과는 관계없이 유지보수 비용이 책정되므로 고품질의 유지보수 서비스를 기대하기 어려우며, 현행 법으로는 적정한 SW 유지보수 사업비를 산출하기 어려운 상태이다.

현행 SW 유지보수 대가산정 기준은 정보보안 SW에는 맞지 않으므로, 현실에 맞는 적절한 정보보안 SW 유지보수 대가 산정 기준이 필요한 실정이다. 즉, 정보보안 SW 유지보수의 규모와 유지보수 생산성에 영향을 미치는 제반요소를 발견하고, 이들을 비용에 연결시키는 정보보안 SW 유지보수 대가기준의 마련이 필요하다 볼 수 있다. 이는 현실적인 정보보안 SW의 유지보수 요율 기준 수립이 필요하며, 일반 SW의 기준인 기능점수 산정 방식이 아닌 정보보안 SW에 맞는 산정 방식 및 CC인증 등과 같은 외부요건에 대한 비용을 대가 산정에

추가할 필요가 있다.

이에 본 연구는 정보보안SW의 유지보수의 특수성에 대한 분석을 통하여 보안업데이트, 모니터링·로그분석 및 정책 지원 등 추가적인 서비스 지원 등에 대한 유지보수 비용 산정하고 일반 SW와의 원가 비교 분석 조사를 통한 적정유지보수 요율을 도출하고자 한다. 또한, 정보보안 SW 유지보수 대가 구조분석 및 해외 사례 수집 분석을 통하여 정보보안 SW의 유지보수 대가 산정에 대한 기준의 도출이 필요하다.

이를 통해 정책적으로, 정보보안SW의 유지보수 대가를 명확하게 산정하기 위한 S/W 대가기준을 수립하고 사용자 및 공급자에게 적정한 대가 지급 기준을 수립함으로써, 정보보안 SW기업의 경쟁력 향상을 도모하고자 한다.

2. 정보보안 Software 산업 현황

2.1. 일반 SW 산업 유지 보수 현황

국내 SW산업의 시장 환경은 패키지SW, 그룹Ware부문, 사무용SW부문, ERP 부문 등으로 나뉘어져 있으며, 패키지SW부문은 운영체제의 MS, 네트워크 관리의 IBM, DBMS의 오라클과 같은 몇몇 대기업들이 시장을 지배하고 있다. 그에 반해 그룹Ware를 위시한 부분은 언어 장벽과 한국 특유의 기업 문화로 인하여 한국 기업이 비교적 높은 시장 점유율을 확보하고 있는 실정이다.

IDC(2005)는 SW 산업구조를 6가지로 구분하고 있으며, 다음 [표 1]과 같다.

[표 1] SW 산업의 구조

Customer Segment	Publishers	SW brokers
Large Enterprise	Solution suites	Enterprise business process brokers
SMB	Application specialists	Domain brokers
Consumer & Community	Open source & Components	Converged HW / SW / Service

SW 유지 보수란 사용자에게 SW를 제공한 후 발생하는 오류 수정, 기능 수정 및 Up Date를 사용환경이 변화함에 따라 SW를 바꾸는 행위를 말하며, SW의 Life cycle의 일부에 속한다. 소프트웨어 개발 이후에 이루어지는 개선 및 서비스(Evolution and Service) 영역은 크게 운영, 유지보수, 사용자 지원, 재개발로 나눌 수 있고, 그 중에서 유지보수의 유형은 크게 기능 변경과 비기능 변경으로 나눌 수 있다.

2008년에 대기업들의 글로벌 ERP를 구축하였고, 서비스 산업, 교육기관들에게 ERP 도입을 확산되어 기업용 SW시장이 증대 되었으며, 통신 SW수요 증가, 공개SW확대, 개인과 중소기업을 중심으로한 SaaS(Service as a Software)기반 SW 확대로 인하여 SW생산액이 전년 대비 약 5.3% 증가한 3조 4천억 원 규모로 성장하였다. 다음 [표 3]은 국내 SW 시장 규모 추이를 제시한 것이다.

[표 2] SW 유지보수 활동

SW 유지 보수 활동		주요 내용
기능 변경 정의(43%)		기존 SW의 기능을 변경하거나 개선 기존 SW의 기능을 구현하는 컴포넌트나 알고리즘을 대체 비즈니스 Rule의 추가나 변경 외부 도입한 SW의 기능 변경 Data process의 추가나 재전송 시 예외 처리 방식의 변경
비 기능 변경	성능개선(4%)	알고리즘, 구성요소 대체, 변경
		서비스 정지의 지속시간 변경
		실행속도 변경
	코드 정비(3%)	주석 처리, 수정, 추가
		권한 변경, 사용자 보안
		라이브러리 파일 수정
	오류수정(21%)	비즈니스, 룰, 에러 수정
		Data 흐름 수정
		예외 처리 변경
	환경적응(25%)	통신 프로토콜 변경
		Data Base 변경
		상호 운영성 변경
	예방조치(4%)	선 조치를 통한 향후 유지보수 방지

[표 3] 국내 SW 시장 규모 추이

[단위 : 억 원]

구분	2006년	2007년	2008년
패키지 SW	32,148	32,547	34,271
IT 서비스	178,468	186,350	198,040
합계	210,616	218,897	232,311

2.2. 정보보안 SW 산업

한국인터넷진흥원(2010)은 정보보안 SW를 “정보의 수집·가공·저장·검색·송신·수신 중에 정보의 훼손·변조·유출 등을 방지하기 위해 구동되는 SW”로 정의하였다.

‘information security’는 정보보호 또는 정보보안을 의미함. 정보보안은 사람에 의하여 고의적으로 발생하는 정보의 유출, 파괴, 변조에 대한 대응을 강조하며, 정보보호는 고의적인 침해 뿐 만 아니라

우연히 발생하는 자연재해나 사람의 실수에 의한 침해에 대한 대응도 포괄하는 포괄적인 용어이다. Security라는 용어가 information과 결합될 때는 정보보안이라는 용어보다는 정보보호라는 용어를 주로 사용하며, 정보보호기술 표준용어로는 정보보호가 사용되고 있다.

정보보호는 국가별로 여러 가지 형태로 정의되고 있는데, 국내의 경우에는 정보화촉진기본법 제 2조에 '정보의 수집, 가공, 저장, 검색, 송신, 수신 중에 정보의 훼손 변호 유출 등을 방지하기 위한 관리적 기술적 수단을 강구하는 것'으로 정의하고 있다.

정보보안 산업 제품에 대한 분류는 다음 표와 같으며, 본 보고서에서는 가장 최신 자료인 '2009 국내 지식정보보안산업 시장 및 동향 조사'에서 활용한 표준 분류체계를 적용하였다.

'정보보안 서비스'는 세부적으로 유지보수, 보안컨설팅, 보안관제, 인증서비스, 기타서비스의 5가지로 구분하며, [표 4]에 제시되어있다.

[표 4] 정보보안 서비스 제품 분류

대분류	소분류	기호	세부 항목
정보보안 서비스	유지보수	O	1 판매 후 유료서비스
	보안컨설팅	P	1 인증(ISO, ISMS) 2 안전진단/기반보호 3 진단 및 모의해킹 4 개인정보보호 5 종합보안컨설팅
	보안과제	Q	1 보안관제 서비스
	인증서비스	R	1 공인/사설 인증서비스
	기타서비스	S	1 교육 훈련 서비스 2 기타

정보보호는 정보의 기밀성(Confidentiality), 무결성(Integrity) 및 시스템의 가용성(Availability)을 보장하기 위한 것으로, 정보화 사회로 발전하는 데 있어 정보화와 동시에 진화해야 할 개념이다.

정보보안 Software Lifecycle은 2009년에 제시된 Microsoft 정보보안 개발 생명주기(SDL : Security Development Lifecycle) 방법론을 중심으로 알려졌다.

Microsoft 정보보안 방법론은 정보보안 SW의 구축 및 유지보수를 위한 절차를 제시하고 있으며, Pre-SDL(교육) 단계, 요구사항 단계, 설계 단계, 구현 단계, 검증 단계, 릴리즈 단계, Post-SDL(대응) 단계로 구성되어 있다.

정보보안 SW의 유지보수 대가 산정 기준을 위해서는 정보보안 SW의 SDLC를 분석하고 보안 검증 절차에 대한 프로세스 및 활동에 대한 분석을 실시함으로써 단계별/영역별/기능별 유지보수 대가 산정 기반을 마련할 필요가 있으며, 본 방법론은 정보보안 SW의 SDLC를 명확하게 제시하고 있으며, 지속적인 유지보수를 위한 절차를 제시한다.

한국인터넷진흥원(2010)은 정보보안 SW 유지보수를 "정보보안 SW을 최적의 상태에서 활용·유지하기 위해 제공되는 제품지원, 기술지원 및 사용자 지원 서비스"로 정의하고 있으며, 정보보안 SW 하자보수의 정의를 "정보보안 SW 자체의 오류 및 결함에 대한 수정을 말하며, 설계 및 코딩 상의 오류 수정, CD 미디어 교환, 온라인을 통한 버그 패치"로 정의하고 있다.

정보보안 SW 유지보수 서비스 항목의 구분 기준은 지원 성격 및 방법에 따른 구분과 지원 매체에 따른 구분으로 나눌 수 있다. 지원 성격 및 방법에 따른 구분은 제품관련 서비스, 기술지원 서비스, 교육이 해당하며 지원 매체에 따른 구분은 전화, 온라인, 방문지원 등을 포함한다.

지원 성격 및 방법에 따른 서비스 항목은 제품관련 서비스, 기술지원 서비스, 교육서비스가 있다.

3. 정보보안 SW유지보수 현황

3.1. 국내 정보보안 SW 유지보수 현황

현재, 국내 기업의 유지보수 서비스 사업은 전체 SW계약금액의 13%를 차지하고 있으며, 일반적으로 알려진 H/W의 유지보수요율(9~10%)과 비슷한 수준으로 지속적인 제품 업그레이드 및 커스터마이징, 교육·훈련의 서비스가 유지되어야 하는 S/W의 유지보수 서비스 요율이 단순 하자보수 서비스를 주로 하는 H/W의 요율 수준과 비슷하다는 것은 S/W 관련 서비스의 인식이 낮다는 것을 보여주는 예라고 할 수 있다.

국내 연매출 100억 원 이상의 주요 정보보호 SW 9개사를 대상으로 지난 2006년부터 2009년 4월까지의 유지보수 요율 실태를 조사한 결과(전자신문,2010), 국내 공공 부문 정보보호 SW 유지보수 요율은 평균 7.8%, 대기업과 금융권을 포함한 민간 부문은 10.3%에 불과한 것으로 파악된다.

또한, 제품 공급가의 10% 안팎인 국내 업체의 유지보수율은 22% 안팎인 외국 업체의 요율에 비해 턱없이 낮은 수준이며, 9개 정보보호업체 모두 공공

부문의 SW 유지보수요율이 민간 부문의 그것보다 낮은 수준으로 파악된다.

3.2. 미국 정보보안 SW 유지보수 현황

미국은 제품의 하자보수를 중심으로 하는 기본적인 유지보수 업무외에 기술지원 서비스 업무를 패키지화하여, 사용자와 공급자간 SLA(Service Level Agreement)를 통해 도입가의 평균 20-30%에 해당하는 유지보수 계약을 체결하고 있다.

오라클, SAP 등 글로벌 컴퍼니의 경우 22%의 SW 유지보수 요율로 계약을 체결하고 있다.

미국 내 정보보안 비용 추정 지침은 보안 제어 실행과 보안 수준 및 비용과 관련된 예산 책정과 관련하여 교육부를 돕기 위해 설계되었으며 'NIST SP 800-26: *Security Self Assessment Guide for Information Technology Systems'* 과 관련하여 관리 기반의 특정 보안 제어, 운영적 기술적 제어에 대한 기준을 제시한다. 각 업무별로 비용을 세 부문으로 분류하고, 기간별 비용 기준 및 소요 기간을 제시하고 있다.

3.3. 일본 정보보안 SW 유지보수 현황

일본은 IT기술 영향력의 증대, 보안 관련 피해 증가, 정보보안에 관한 구체적 기준이 존재 하지 않은 현실에 따른 사회적 요구의 증가에 따라 정보보안 기준 제시의 필요성이 대두되었다.

이러한 문제를 해결하기 위해 우선적으로 해외사례 분석(미국, 영국, 한국 등)을 통하여 정보보안에 관한 구체적 기준을 제시하고자 하였으며, 중점적으로 영국OGC(Office of Government Commerce)의 정보서비스에 관한 "베스트 프렉티스"와 미국의 NIST의 보고서를 참조하였다.

현재 일본에서 적용하고 있는 정보보안 관련 주요 가이드라인은 다음 [표 5]와 같다.

[표 5] 일본 정보보안 관련 주요 가이드라인

구분	가이드라인 명칭
경제 산업성	정보 시스템에 관한 정부 조달을 위한 SLA도입 가이드 라인
총무성	공공(公共)의 IT 아웃 소싱에 관한 가이드라인
전자 정보 기술 산업 협회	민간을 위한 IT 시스템의 SLA 가이드라인

現 제시 가이드라인은 미국과 영국의 정보보안 추진 방식인 SLA를 중심으로 전자정부를 구축하는 것을 목적으로 한다.

제시한 정보보안 가이드라인을 구현하기 위해, 일본 내 정보보안 현황 파악을 위한 "정보 시큐리티 사고에 관한 조사"로 불리우는 선행 조사가 이루어진 것을 보더라도 정보보안의 중요성을 인식하고 있는 것으로 사료된다.

4. 결론

본 연구는 문헌연구, 실태조사, 국내·외 사례조사 및 인터뷰를 통하여 정보보안 S/W 유지보수 사업 분야에 대한 관련이슈를 도출하고, 이슈를 통하여 정보보안 S/W 대가산정 기준을 수립하기 위한 개선방안을 도출하고자 하였다.

정보보안SW는 일반SW 유지보수에 비해 보안 정책 지원 등 추가 서비스를 수행하나, 추가 서비스에 대한 대가는 따로 산정되지 않고 있으며 업데이트마다 이루어져야 하는 CC(국제공통평가기준)인증 비용도 고려되지 않고 있다. 그리하여 추가적인 서비스 지원 등에 대한 유지보수 비용 산정하고 일반 SW와의 원가 비교 분석 조사를 통한 적정유지보수 요율을 도출하고자 한다.

후에 설문조사, 요율 체계 분석 시뮬레이션, 대가 산정/검증, 전문가 검증을 통해 정책적으로, 정보보안SW의 유지보수 대가를 명확하게 산정하기 위한 S/W 대가기준을 수립하고 사용자 및 공급자에게 적정한 대가 지급 기준을 수립함으로써, 정보보안 SW기업의 경쟁력 향상을 도모하고자 한다.

참고문헌

[1] 김세헌, 「정보보호 관리 및 정책」, 생능출판사, 2002
[2] 인터넷진흥원(KISA), 국내 정보보호산업 시장 및 동향조사, 2009, p.15-16
[3] 일본 총무성, 공공의 IT 아웃 소싱에 관한 가이드 라인, 2003, 3
[4] 정보통신부 제정, ' 패키지SW 유지보수 서비스 가이드라인'전문, 2005. 05
[5] 정보 통신 정책 연구원, SW산업 활성화를 위한 법·제도 정비방안에 관한 연구, 1999. 12.
[6] 정부연, "제 1절 소프트웨어", 정보통신 산업동향, 2008.12
[7] 한국전산원, "소프트웨어 유지보수 대가기준 모형 연구", 2004.10
[8] Department of Education, United States of America, Information Technology Security Cost Estimation Guide, 2002
[9] KAIT 정보통신 통계연보 2007, 2008년 KISDI 예측치
[10] Regents of the University of Minnesota, IT Service Level Agreement, 2009