EWBS를 통한 정보보호 시스템의 보안성 평가 업무량 및 비용 산정 프로세스

(An Estimation Process of Effort and Cost in Security Evaluation of Information Technology Security Systems by utilizing Evaluation Work Break-down Structure)

유 형 준 † 고 정 호 † 장 수 진 †† 안 선 숙 †††

(Hyung-Joon You) (Jeong-Ho Ko) (Soo-Jin Chang) (Sun-Suk Ahn)

이 강 수 †††† 정 홍 진 †††††

(Gang-Soo Lee) (Hong-Jin Jung)

요 약 국·내외적으로 소프트웨어 산업이 활성화되었음에도 불구하고, 정보보호 소프트웨어 시스템의 보안성 평가를 포함한 각종 소프트웨어의 품질 평가 업무량 및 평가 비용 산정에 대한 연구는 부족하다.

본 연구에서는 업무분해구조(EWBS) 방법과 기존의 소프트웨어 개발비 산정 방법을 응용하여, 정보보호 시스템의 평가기준(Common Criteria 또는 ISO/IEC 15408)에 따라 정보보호 시스템을 평가 할 때의 평가 업무량과 평가 비용을 산정하는 프로세스와 도구를 제시한다. 본 연구는 정보보호 시스템의 평가 업무량과 평가 비용의 산정에 중심을 두고 있지만, 본 연구의 결과는 기존의 소프트웨어 개발 프로세스 및 제품의 품질 평가시의 평가 업무량 및 평가 비용의 산정에도 응용될 수 있다.

Abstract Even though software industry has been activated, there lack in results of studies on evaluation effort and cost of software systems including Information Technology Security System (ITSS).

In this paper, we present a process and a tool for evaluation effort and cost of ITSS, which are conformed to a ITSS evaluation criteria(i. e., Common Criteria or ISO/IEC 15408), by utilizing Evaluation Work Break-down Structure (EWBS) and conventional software development cost estimation methods. Even though we concentrate on ITSS, results of this paper can be applied to estimation of effort and cost of evaluation of software development process and software products.

· 본 연구는 한국학술진흥재단(98년 자유공모과제)과 한국정보보호센터의 지원으로 연구되었음

† 학생회원 : 한남대학교 컴퓨터공학과
youhj@se.hannam.ac.kr
jhko@sc.hannam.ac.kr
†† 비 회 원 : 대전보건대학 전산정보처리과 교수
sjjang@thealth.ac.kr
††† 비 회 원 : 한남대학교 회계학과
ssan@kebi.com
†††† 종신회원 : 한남대학교 컴퓨터공학과 교수
gslee@eve.hannam.ac.kr
††††† 비 회 원 : 한남대학교 회계학과 교수
hjchung@eve.hannam.ac.kr

논문접수 : 1999년 5월 3일
심사완료 : 1999년 12월 1일

1. 서 론

컴퓨터는 네트워크의 일부로 변하고 비즈니스 영역이 광역화됨에 따라, 소프트웨어들간의 호환성 및 상호 운용성을 높이기 위해, 소프트웨어의 구조(예; CORBA, DCOM/OLE 등), 기능(예; TCP/IP, MPEG, MIDI 등) 및 자료구조(예; EDIFACT, HTML 및 VRML 등)뿐 아니라, 개발 프로세스 및 제품의 품질에 대한 평가기준도 표준화(예; CMM, SPICE, ISO/IEC 9001, 9126, 14598)되었다[1~4].

S/W 개발자들은 이들 표준에 따라 개발한 후, 개발물의 적합성 시험, 품질 평가 및 인증 활동을 통해 개발물이 표준에 순응함(conformance)을 보인 후 이를 제삼

자(인증기관)를 통해 인증(certification)받을 필요가 있다. 이 경우, 개발자는 순수 개발비 뿐 아니라, 평가 및 인증 비용도 부담해야만 한다. 소프트웨어의 획득자도 최소의 비용으로 최고의 품질을 갖는 제품을 획득하기 위해 제품평가가 필요하다.

따라서, 소프트웨어의 평가 비용(예; 적합성 시험비용, 품질 평가 비용, 보안성 평가 비용, 성능 평가 비용 등)과 인증 비용의 산정이 필요하다. 소프트웨어 개발 및 유지보수 비용의 산정을 위한 연구들[5~8]이 활발하며 국내에서도 '소프트웨어 사업대가의 기준[9]'이 제정 및 공표되어 있다. 또한, 원가계산 부문[5]에서도 공산품의 개발 원가계산에 관한 연구가 활발하다. 그러나, 정보보호 시스템의 보안평가 업무를 포함한 일반적인 소프트웨어의 프로세스, 제품 및 자원의 평가 비용 산정에 관한 연구는 부족하다.

이와 같은 배경에서, 본 논문에서는 정보보호 시스템의 국제 평가기준인 CC(Common Criteria, ISO/IEC 15408)[10]에 따라 정보보호 시스템을 개발 및 평가할 때의 평가 업무량과 평가 비용 산정 프로세스를 제시한다. 본 프로세스에서는 평가기준을 Evaluation Work Break down Structure (EWBS) 방법을 적용하여 단위 평가업무들로 세분화한 후, 단위 평가업무에 대한 난이도를 추정하고 평가용 산출물(deliverable)의 크기를 예측하고 전체 평가 업무량과 비용을 산정한다.

정보보호 시스템의 평가기준들에서는 기존의 소프트웨어 평가모델과는 달리 소프트웨어의 개발 프로세스, 제품 및 자원을 통합적으로 평가하고 있다. 따라서, 본 논문에서 '평가'란 프로세스, 제품 및 자원을 통합한 평가를 의미하며 정보보호 시스템은 정보보호 '소프트웨어' 시스템을 의미한다.

본 논문의 2장에서는 일반 소프트웨어 제품 및 정보보호 제품의 평가 비용 산정과 관련된 연구동향을 보이며, 3장에서는 EWBS에 의한 평가 업무량의 산정 프로세스와 도구를 제시한다. 4장에서는 정보보호 시스템의 평가 업무량과 평가 비용 산정 결과를 보이며 5장에서 제시한 내용의 분석과 함께 결론을 맺는다.

2. 관련 연구

2.1 지식 서비스와 공산품 평가 부문의 원가계산

지식 서비스 부문에서는 고객에게 무형의 서비스를 제공하고 수수료를 받는다. 감사, 영화제작, 연구 과제 및 소프트웨어의 평가 업무도 지식 서비스에 해당하며, 개별 서비스 작업에 소요되는 시간, 소요 자원 및 기술적 복잡성 등은 서비스 원가에 중요한 변수가 된다[8]. 서비스업의 경우 인건비가 큰 비중을 차지하며 소프트웨어의 평가작업도 인건비가 큰 비중을 차지하므로, 평가자의 작업시간 기록이 중요하다(미국 회계법인에서는 각 작업에 대하여 30분 단위로 작업시간을 기록하도록 요구하고 있음).

공산품 평가 부문중 KS표시 허가의 평가 비용 산정 항목은 신청 수수료, 공장 심사 수수료, 제품 시험 수수료 등으로 구분되며, 일부 국가에서는 ISO/IEC 9000과 QS-9000 품질 인증 제도에서도 신청수수료, 평가 및 인증 비용을 고시하고 있다. 이들 비용은 평가의 원가계산을 통해 산정되어 고시된 것들이다.

2.2 소프트웨어 개발비용 산정

B. Boehm은 자신이 축적해놓은 소프트웨어 개발비용 자료와 기존의 연구결과들을 토대로 하여 COCOMO 81을 포함한 "소프트웨어 경제학"을 제시하였다[5]. 초기의 비용모델들은 주로 소프트웨어의 크기를 독립변수로 하여 개발업무량을 예측하고있다. 80년대와 90년대에는 그 동안 축적된 소프트웨어 비용자료를 바탕으로 하고, 객체지향 기술 등과 같은 새로운 소프트웨어 개발기술에 적합한 비용 모델(예; Function Point(FP) 모델)이 등장하였다[6,7]. Boehm의 COCOMO-81모델도 Function Point(FP)모델과 결합하여 COCOMO-Ada 및 COCOMO-2.0[6,7]모델로 진화되어왔다.

COCOMO 81모델[5]은 70년대의 자료를 이용한 15가지 비용유도 속성들의 가중치 또는 승수를 사용하며 예상 크기를 추정해야만 하는 단점이 있으며, 객체지향 기술, 4GL 및 재사용 기술과 같은 신기술에 의한 개발환경을 반영하지 못한다. COCOMO 2.0은 COCOMO-81의 최근 버전으로서 Object Point(Stage 1에서), FP 및 Language(Stage 2에서), FP 및 Language 또는 DSI(Delivery Source Instruction) 모델(Stage 3)로 구성된다[6,7]. COCOMO 2.0은 COCOMO-81과는 달리, 비용유도 속성의 승수들은 매년 수정 및 발표되고 있다.

우리 나라의 경우, 1989년에 DSI형 모델인 COCOMO-81을 변형한 "소프트웨어개발비 산정기준"을 과학기술처에서 고시하였으며, 현재에는 DSI형 모델과 FP 모델을 선택적으로 적용할 수 있는 "소프트웨어사업대가의 기준"을 정보통신부에서 고시하고 있다[9]. 그러나, 기준에는 시험 및 평가에 대한 비용산정 기준은 포함되어있지 않다.

2.3 정보보호 시스템의 평가와 인증 제도

방화벽이나 침입탐지 제품과 같은 정보보호 시스템의 구매자는 第三者에 의해 그 보안 능력을 인증받은 제품을 선호하게되므로, 시스템의 시장 경쟁력을 확보하기

위해서는 시스템의 평가와 인증이 필요하다. 이에 따라, 평가와 인증을 위해 각 국에서 이를 위한 기준들이 적용되고 있다[14]. 80년대 중반부터 90년대 중반까지는 각 국가별로 평가기준을 적용하였으며[11~13], 90년대 후반부터 국제 표준 평가기준이라 할 수 있는 CC를 개발하기 시작하여 1998년 5월에 완성된 CC Version 2.0은 1999년 6월에 ISO/IEC 15408로서 국제 표준화되었다[10]. CC의 평가방법론인 CEM(CC Evaluation Methodology) 버전 1.0[15]은 EAL 4등급까지의 평가방법론을 제시하고있다.

한편, 국내에서도 1990년대부터 정보의 보호 또는 정보화의 역기능을 방지하기 위해 '정보화 촉진 기본법'(법률 제4969호)이 제정되고 '한국정보보호센터'가 설립되었다[14]. CC의 개념을 수용하여 일반적인 정보보호 시스템(예; OS, 접근통제, 컴퓨터 바이러스 방지, 침입탐지, 사용자 인증 제품)들을 평가할 수 있는 '정보보호 시스템 평가기준 0.7' (K-CC라 칭함)을 개발하고 있다[16]. 침입차단(방화벽)시스템의 경우, 평가의 원가계산을 통해 보증수준별 수수료를 고시하고 있지만[17], 일반적인 정보보호 시스템의 평가수수료 산정에 대한 연구는 미비하다.

2.4 소프트웨어 평가기준과 정보보호 시스템 평가기준

소프트웨어 공학 분문에서는 평가를 크게 세가지로 구분하고 있다[1]. 첫째, '제품'의 평가는 Boehm 모델[5], ISO/IEC 9126[2], ISO/IEC 14598[3] 및 Doromy 모델 등을 적용하고 있다. 둘째, 개발 '프로세스'의 평가는 사후(postmortem) 분석, ISO 9001 모델, 미국 SEI의 CMM(Capability Maturity Model), 영국의 SPICE(Software Process Improvement and Capability Determination) 등을 적용하고 있다. 셋째, 개발 '자원'(개발요원을 포함)의 평가에는 PMM(People Maturity Model) 및 투자회수율(Return of Investment; ROI) 등을 적용할 수 있다.

이러한 소프트웨어 품질 평가기준 및 모델들은 소프트웨어의 모든 품질특성들을 평가하기 위한 일반적인 기준이지만 CC[10], ITSEC[11] 및 TCSEC[12,13]과 같은 정보보호 시스템의 평가기준들은 품질 특성들 중 주로 기능성과 보안성을 평가하기 위한 구체적인 평가기준이다. (참고: ISO/IEC 9126에서는 보안성은 기능성 내에 포함되어 있다.)

정보보호 시스템 평가기준들에서는 소프트웨어 평가기준들과는 달리, 프로세스 및 제품의 평가기준이 통합되어 있으며, 보안기능의 평가기준들은 평가 보증수준에 따라 계층구조를 가진다. 또한, 목표 평가 보증수준에 대한 기준들의 만족여부(합격/불합격/유보)를 주로 평가하고 있다. 따라서, 정보보호 시스템의 평가기준들은 기존의 소프트웨어 프로세스 및 제품의 평가기준의 한 '인스턴스'로 간주할 수 있다.

3. 정보보호 시스템의 평가 업무량 산정 프로세스

평가 업무의 대부분은 개발자의 몫이며 그림 1과 같이 개발자는 평가대상물(Target of Evaluation; TOE)을 개발하고 평가에 필요한 산출물을 준비해야한다. 산출물 중 '요구사항 명세서'는 보호프로파일(PP; Protection Profile) 또는 보안목표명세서(ST; Security Target)라 한다. 평가자는 산출물을 근거로 하여 개발과정과 개발환경 등이 정확하며 적절한지를 확인, 체크, 검증 및 독립 시험하는 것이다.

3.1 평가 업무량 모델

정의 1은 본 논문에서 사용하는 용어와 약어들을 보인다.

[정의 1] 평가업무와 관련된 용어와 약어

- FUN = $\{FC_1, ..., FC_i, ..., FC_n\}$: 전체 기능 집합,
- $FC_i = \{fun_{i1}, fun_{ii}, fun_{im}\}$: 기능 클래스
- $min \le j \le max$: 보증 수준 또는 등급(여기서, min, max는 각각 최소 및 최대 보증수준)
- COST(i, j) : i 기능 클래스 제품 FC_i에 대한 j보증수준의 평가비용($cost(i, j)_k \in COST(i, j)$)
- TIME(i, j): i 기능 클래스 제품에 대한 j보증수준의 평가기간 ($time(i, j)_k \in TIME(i, j)$)
- WORK(i, j) : i 기능 클래스 제품에 대한 j보증수준의 평가업무 ($work(i, j)_k \in WORK(i, j)$)
- EFFORT(i, j) : i기능 클래스 제품에 대한 j보증수준의 평가 업무량 ($effort(i,j)_k \in EFFORT(i, j)$) (단위는 unit_workload)
- CRIT(i, j) : i 기능 클래스 제품에 대한 j보증수준의 평가기준 ($crit(i,j)_k \in CRIT(i, j)$)
  (여기서, CRIT(FUN, max)는 모든 기능클래스 제품의 최상위 보증수준 평가기준(즉, 전체 평가기준)을 나타냄)
- TOOL(i, j) : i 기능 클래스 제품에 대한 j보증수준의 평가도구 및 사용량($tool(i,j)_k \in TOOL(i, j)$)
- DIFF(i, j) : i 기능 클래스 제품에 대한 j보증수준의 평가 난이도($diff(i,j)_k \in DIFF(i, j)$)
- DLV(i, j) : i 기능 클래스 제품에 대한 j보증수준의 평가를 위한 산출물 ($dlv(i,j)_k \in DLV(i, j)$)

보증수준 또는 보증등급은 자동차의 에너지 등급, 대학

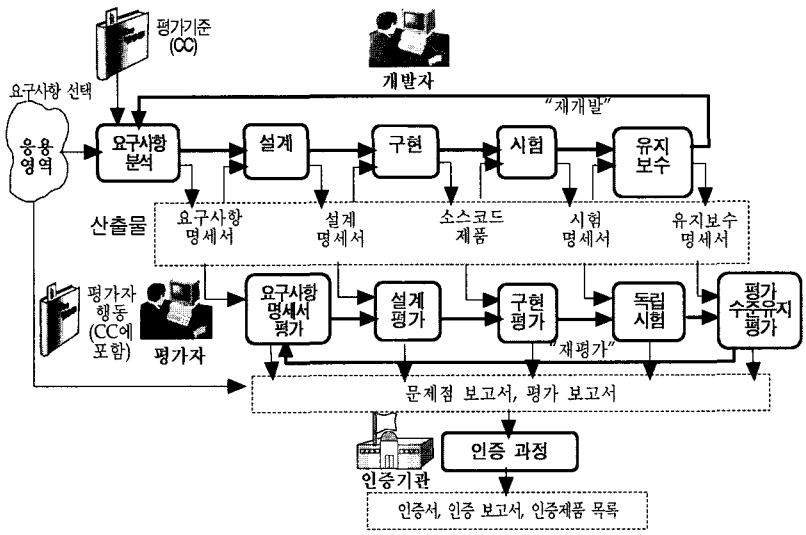


그림 1 정보보호 시스템의 개발 및 평가 프로세스간의 관계

평가 등급, 신체장애 등급 및 품질 등급처럼 등급별 평가기준(즉, 기능의 보장성)의 만족여부를 나타내며 속성 1처럼 상위등급은 하위등급을 포함하고있다.

[속성 1] 보증수준의 단조증가성(monotinicity)

For $\forall i \in CLASS$, $COST(i, j) < COST(i, j+1)$,
$EFFORT(i, j) < EFFORT(i, j+1)$,
$CRIT(i, j) \subset CRIT(i, j+1) \subseteq CRIT(FUN, max)$,
$TOOL(i, j) \subset TOOL(i, j+1)$,
$DIFF(i, j) < DIFF(i, j+1)$, $DLV(i, j) \subset DLV(i, j+1)$

어떤 평가기준(예; CC)에서 기능클래스가 FC_i (예; 운영체제)이며, 목표 평가수준 j수준(예; EAL4)에 대한 평가기준 전체는 그림 2와 그림 3과 같이 "단위 평가기준"들로 분해(breakdown)할 수 있으며, 평가대상물에 대한 평가용 전체 산출물도 "단위 산출물"로 분해할 수 있다. 또한, 전체 평가환경(평가자 및 도구)도 "단위 평가환경"으로 분해할 수 있다. 따라서, 평가를 위한 "단위 평가업무"는 이에 대응하는 평가기준, 산출물 및 평가환경의 함수이며, j수준의 "평가 업무량" $EFFORT(i, j)$는 j수준의 단위 평가업무 $work(i, j)_k$들의 "단위 평가업무량" $effort(i, j)_k$의 합이 된다. 또한, 단위 평가 업무량은 해당 단위 평가업무를 위한 산출물의 크기, 평가난이도 및 도구 사용량으로부터 구할 수 있다.

3.2 평가 업무량 산정 프로세스

(1) EWBS에 의한 단위 평가업무 work(i, j)k 분석

평가기준(또는 산출물, 평가환경)의 계층적 구조인 '클래스 - 컴포넌트 - 요소 - 단위'는 평가업무의 EWBS인 '평가활동(activity) - 평가부활동(sub-activity) - 평가행동(action) - 단위업무(unit work)'로 각각 대응시킨다.

- 평가기준의 스키마(즉, 평가기준 문서의 목차 및 구조에 해당)를 계속적으로 분해하여 '단위 기준'을 구한다. 단위 기준은 더 이상 분해할 수 없으며, 단순 명제(simple predicate) 또는 단순 술어(simple proposition) 형태가 되며 '단위 업무'와 대응시킨다. 단위 기준과 단위 업무는 1 : 1관계가 된다.
- 산출물을 분해하여 '단위 산출물'들을 구하고 이들을 단위 업무들과 대응시킨다. 단위 산출물과 단위 업무들간에는 n : m 관계가 된다.
- 평가환경(평가자 및 도구)을 분해하여 "단위 환경"들을 구하고 이들을 단위 업무들과 대응시킨다. 단위 환경과 단위 업무들간에는 n : m 관계가 된다.

(2) 단위 산출물 크기 Size(dlv(i, j)$_k$) 산정

이들 업무의 평가 업무량은 산출물의 크기에 비례한다. 예컨대, 개발자가 검증이나 시험을 많이 했다면 산출물(예; 시험보고서)의 크기도 길어지며 평가자도 이에 비례하여 검증 및 독립 시험 업무를 수행한다. 또한, 대부분의 소프트웨어 개발비용 예측 모델에서는 개발될예상 소스코드 크기(또는 길이) 값을 주로 이용한다

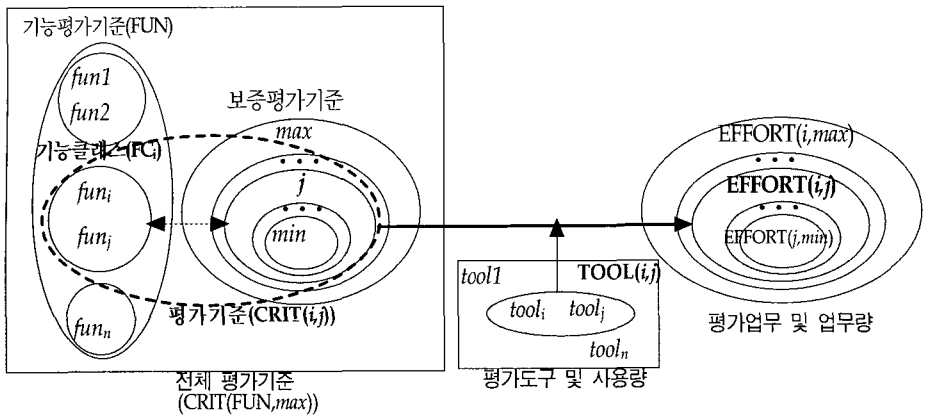


그림 2 정보보호 시스템의 평가기준과 평가 업무량과의 관계

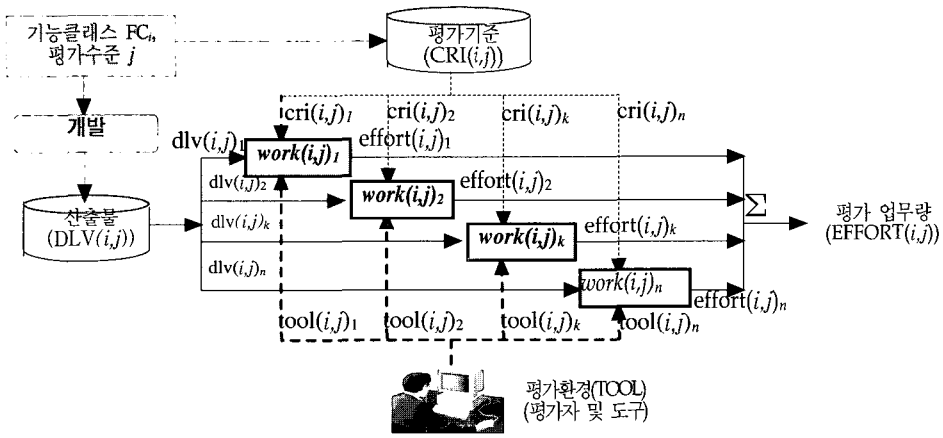


그림 3 정보보호 시스템의 평가업무와 평가 업무량과의 관계

[5,6,7]. 즉, 소프트웨어의 크기가 개발비에 큰 영향을 미치기 때문이다.

따라서, 본 연구에서도 평가에 필요한 산출물의 크기를 추정하여 이를 평가 업무량 산정에 이용한다. 산출물 크기 산정시의 불확실성을 줄이기 위해 '베타분포'를 사용하였다. 베타분포는 프로젝트 관리 분야에서 주로 사용되는 확률분포 함수로서 인간의 행동과 시간의 불확실한 면을 잘 나타낸다. 베타분포 함수로부터 $dlv(i, j)_k$의 최선의 예측 크기, 중간 예측 크기 및 최악의 예측 크기를

각각 a, m 및 b라 할 때, $Size(dlv(i, j)_k) = \mu = (a + 4m + b)/6$,

$variant(dlv(i, j)_k) = [(b - a)/6]$ 이 된다.

(3) 단위 평가업무별 난이도 $diff(i, j)_k$ 결정

① 단위 평가업무들을 유형별로 분류 : 체크(예; 표본, 전체), 확인(confirm) (예; 산출물과 증거 요구사항간의 만족성, 적용성, 순응성, 부분결과, 선택적 검증, 분석결과, 정확성, 일관성, 준수성, 범위, 수행), 결정(determine) (예; 구성여부, 실현여부, 내성, 종속관계), 시험(test) (예; 부분, 시험결과의 표본, 시험결과의 전체, 독립시험, 침투시험), 재현(예; 설치, 기타), 취약성 분석, 문서의 스타일 평가

② 각 유형에 대한 상대적 난이도 결정 : 체크 < 확인 < 결정 < 재현 < 시험 < 취약성분석 (여기서, a <

b를 b는 a보다 난이도가 높으며 평가 업무량이 많음으로 정의)

③ 결정한 난이도의 개선 : 기존의 의사결정 이론과 평가경험을 활용하여 난이도를 계속 수정함

여기서, 난이도의 결정은 평가자의 능력과 평가환경에 따라 달라질 수 있으며 평가 경험과 관련자료(예컨대, COCOMO의 소프트웨어 개발노력량에 영향을 주는 속성들의 가중치 등)로부터 유추할 수 있다.

(4) 전체 평가 업무량 EFFORT(i, j) 산정

각 단위평가업무에 대응하는 평가도구의 사용량 TOOL$(i, j)_k$ 를 조사하여 다음 식에 의해 전체 평가 업무량을 구한다.

$$\mathrm{EFFORT}(i,j) = \mathit{Size}(\mathrm{DLV}(i,j)) \times \mathrm{DIFF}(i,j) + \mathrm{TOOL}(i,j) + \sum_k [\ \mathit{Size}(\mathrm{dlv}(i,j)_k) \times \mathrm{diff}(i,j)_k + \mathrm{tool}(i,j)_k]$$

(5) 업무량의 상대적 비율 REL(k, l) 산정

업무량의 상대적 비율은 REL(i, j)을 기준 업무량이라 할 때, 다음과 같이 계산한다.

$$\text{For } \forall k, l,\ 1 \le k \le n,\ \min \le l \le \max,\ k \neq i,\ l \neq j,$$
$$\mathrm{REL}(k,l) = \mathrm{EFFORT}(k,l) / \mathrm{EFFORT}(i,j)$$

여기서, COST들 중 이미 알려진 것이 있을 때 이를 기준업무량으로 정한다.

(6) 기초 평가비 산정 및 정산

'기초 평가원가'란 평가에 소요되는 원가이며 여기에 10%의 이윤(참고: 국가를 당사자로 하는 계약에 관한 법률 시행 규칙의 제 8조에 의하면, 용역의 경우 이윤은 직접비와 일반 관리비의 합계액의 10%를 초과하지 못함)을 포함하면 '기초 평가비'가 된다. 공공 기관의 경우 이윤은 계상할 수 없으므로 기초 평가원가와 기초 평가비는 같다. 기초 평가비와 평가기간은 다음과 같이 계산된다.

$$\mathrm{COST}(i,j) = \mathrm{EFFORT}(i,j) \times \mathrm{unit\_cost}$$
$$\mathrm{TIME}(i,j) = a \times \mathrm{EFFORT}(i,j)^b \quad (a,\ b\text{는 계수})$$

소프트웨어의 개발 업무는 평가나 개발 환경의 특성(예; 평가자의 능력, 소스코드크기 등)에 따라서 '실질 평가비'가 달라진다. 따라서, 평가의뢰자는 평가 시작시에 '기초평가비'를 지불한 후, 평가 실시 후 평가환경을 고려하여 실제 평가비를 계산하여 그 차액을 정산해야 한다.

본 연구에서는 COCOMO-II [6,7]에서 사용하는 22가지의 소프트웨어 개발환경 속성을 응용하여 다음과 같이 실제의 평가환경 속성 승수 MULT를 구한 후 평가비의 정산액을 구한다[26].

$$\mathrm{MULT} = \prod_{i=1}^{22} \mathrm{ATT}_i$$

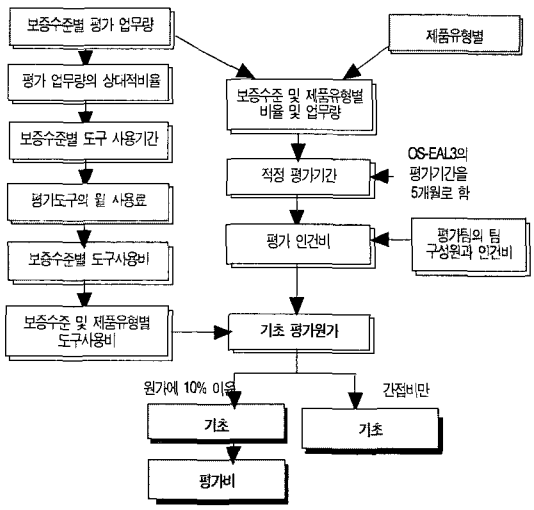
정산액 = |기초평가비 − 기초평가비×MULT|

(여기서 ATT_i = 1(평균적일 경우), $0 < \mathrm{ATT}_i < 1$ (우수할 경우), $1 < \mathrm{ATT}_i < 2$ (열악할 경우)

평가 업무량 EFFORT(i, j)와 도구 사용량 TOOL(i, j)은 각각 인건비와 도구 사용비가 된다. 인건비 단가 및 도구 구입비는 평가 기관마다 다르며 매년 노임 단가가 새롭게 고시된다[18]. 따라서, 기초 평가원가는 매년 또는 각 기관마다 달라질 수 있다.

3.3 평가비 산정 도구

제시한 프로세스는 Excel 97로 구현하였으며 정보보호 시스템을 포함한 각종 평가비 산정시, 각종 변수의 변동에 따라 단계별로 자동적으로 재계산하여 평가 비용을 산출해준다. 그림 4는 본 산정 도구내의 각 쉬트들 간의 자료흐름을 보이며 쉬트에 수록된 기본 자료들은 본 연구에서 산정한 자료이며, 평가기준이 변화되거나



(주) 진한부분은 사용자가 입력할 수 있는 쉬트임

그림 4 평가비 산정 도구의 쉬트간의 자료흐름

평가 환경이 변화될 때(예; 평가도구, 평가자 임금, 산출물 크기, 평가 난이도 등), 해당 쉬트 내의 자료를 수정한 후 재수행하면 된다.

4. CC에 의한 정보보호 시스템 평가업무량 산정결과

CC는 500쪽에 이르는 방대한 기준이며[10], 평가방법론 지침인 CEM 1.0도 400쪽 이상으로 구성되어 있다[15]. CC는 일반모델, 보안기능 요구사항 및 보증 요구사항으로 구성되어 있으며 K-CC는 CC의 부분집합이라 할 수 있다. 본 장에서는 CC를 평가기준 사용할 때, 3장에서 제시한 프로세스를 적용하여 정보보호 시스템의 평가노력량을 산정한 과정과 결과를 보인다.

4.1 EWBS에 의한 평가업무 분석

그림 5는 CC의 구조와 EWBS간의 관계를 보인다. CC에서의 각 기능 패밀리와 컴포넌트의 세부 기능 수는 해당 기능의 업무량을 산정할 때 사용했으며, 표 1은 전체 기능수(즉, FUN의 원소수)와 현재 발표된 보호프로파일(PP)들[18~23]과 K-CC[16]에서 선택한 기능수를 보인다. 여기서, OS제품군의 평균 기능수는 65.5개(=(66+65)/2)이며, 방화벽 및 접근통제 제품군의 평균 기능 수는 42개(=(44+40+46+33+42+46)/6)이다. 즉, OS 제품군은 기능면에서 방화벽보다 1.55배(=65.5/42)가 복잡하며 CC의 전체 기능 요구사항내의 세부기능수의 25.9% (=65.5/252) 정도만을 구현하고 있다.

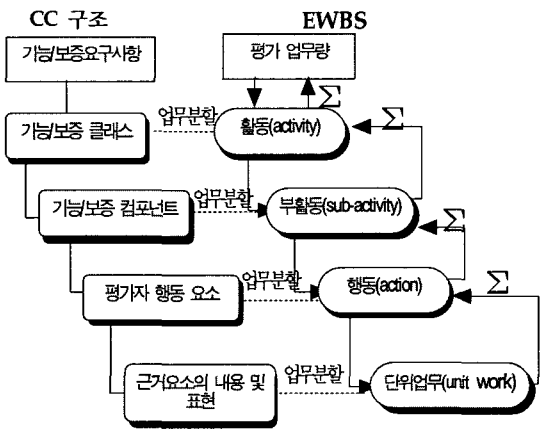


그림 5 CC의 구조와 EWBS

표 2는 보증 요구사항의 보증수준별 각종 개수를 보인다. 이 개수는 보증 요구사항의 평가 업무량으로는 볼 수 없다. 왜냐하면, 각 세부사항의 평가 업무마다 난이도가 다르기 때문이다.

4.2 산출물 크기 산정

다음 과정을 통해 산출물의 크기를 산정하였다.

① CC의 보증 요구사항내의 "개발자 행동"을 바탕으로 하여 평가에 필요한 산출물의 종류와 세부 목차를 구함

표 1 사례 PP 및 K-CC의 제품별 기능 요구사항에서 사용하는 세부 기능수

	항목	기능 패밀리수	세부기능수	CC전체기능과의 비율(%)
	CC 의 기능요구사항	67	252	100
기발표된 PP 자료	레이블된 보안(OS) [19]	25	66	26.2
	제어된 접근통제 [20]	21	44	17.5
	응용수준 방화벽(접근통제) [21]	17	40	15.9
	트래픽 필터형 방화벽 [22]	18	33	13.1
	역할기반 접근통제 [23]	23	42	16.7
K- CC [16] (최고 보증수준의 경우)	인증	14	40	15.9
	접근통제	17	46	18.3
	바이러스 치유	5	11	4.4
	침입탐지	6	18	7.1
	OS	21	65	25.8

표 2 보증 요구사항 각종 세부 사항수 총괄표

보증수준(EAL) / 항목	EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
클래스수	5	6	7	7	7	7	7
패밀리수	7	12	17	23	25	25	25
컴포넌트수	7	12	17	23	25	25	25
단위기능/업무수 (추가 업무수)	23 (0)	44 (1)	61 (3)	93 (6)	109 (14)	131 (20)	134 (31)
개발자 요구사항수	7	16	22	33	39	42	44
증거 요구사항수	23	44	61	93	109	131	134
평가자 요구사항수	10	19	27	39	45	46	48

② 각 산출물내의 세부 내용별로 개발자(또는, 평가의뢰자)가 작성해야할 문서의 크기를 산정(베타분포를 이용함)

③ 세부 내용의 크기를 합하여 전체 크기를 산정함

표 3은 CC의 보증요구사항 평가용 산출물의 목록 및 크기 산정 결과를 보인다. 부록 A에서는 보증수준별 산출물의 크기 산정 결과를 보이며, 부록 B에서는 크기 산정과정의 예로서 형상관리 클래스의 평가용 형상관리 보고서의 크기 산정과정의 일부를 보인다.[25]

표 3 CC 평가용 산출물 목록 및 크기 산정 결과

보고서명	최대 크기(쪽)	용도
형상관리 보고서	40.1	형상관리 클래스 전체
배포와 운영 지침서	10.7	배포와 운영 클래스 전체
기능명세서	17.7	개발:기능명세 및 표현 일치성 패밀리
상위설계서	24.6	개발: 상위 수준 설계 및 표현 일치성 패밀리
구현명세서	3+소스 코드	개발: 구현 및 표현 일치성 패밀리
구조명세서	19	개발: TSF내부 및 표현 일치성 패밀리
하위 설계서	27.9	개발: 상위 수준 설계 및 표현 일치성 패밀리
보안정책 명세서	19	개발: 보안정책 패밀리
설명서	31	설명서 클래스
생명주기 지원 명세서	30.4	생명주기 지원 클래스
시험보고서	52.7	시험 클래스
취약성 분석서	61.2	취약성 평가 클래스
보증의 유지 보고서	47	보증의 유지 클래스

본 연구에서 산정한 산출물의 크기 값을 의무화한다면 다음과 같은 장점이 있다. 첫째, 개발자(또는, 평가의뢰자)와 평가자의 문서에 대한 부담(즉, 작성 및 독해 시간)을 줄일 수 있으며, 둘째, 산출물 작성시 제한된 크기에 맞도록 내용을 압축해야하므로, 문서의 정형성이 높아지고 정보의 전달량이 많아진다.

4.3 평가업무의 평가 난이도 산정

CC 2.0에서는 각 평가기준들에 대해 29가지의 평가자 행동요소들이 제시되었으며, 이들은 검사(check), 확인(confirm), 결정(determine), 시험(test), 반복(재현), 취약성 분석 및 문서의 스타일 등으로 구분할 수 있다. 표 4에서 가정된 난이도들은 CC의 평가기준들에 공통적인 평가자 행동요소인 '산출물과 증거 요구사항간의 만족성 확인'의 난이도를 1로 가정했을 때의 상대적인 난이도이며, ITSEC의 평가지침서인 ITSEM[24] 등의 내용(보안 강도 결정규칙에서, 중간내성은 낮은 것의 2.64배, 높은 내성은 4.36배)을 바탕으로 한 것이다.

부록 C에서는 가정된 평가자 행동 요소별 난이도를 이용하여 보증수준별 보증평가 패밀리들의 난이도를 산정한 과정을 보인다.

4.4 평가업무량 및 업무량의 상대적 비율 산정

표 5는 산출물의 크기, 난이도 및 도구 사용율을 이용하여 각 제품기능유형(i) 및 보증수준(j)에 대한 EFFORT(i, j)값을 보인다. 여기서, 제품 유형은 K-CC

표 4 평가자 행동의 난이도(가정)

평가자 행동유형	세부 행동	난이도
검사	표본 검사	0.5
	모두 검사	0.7
확인 (충족여부)	산출물과 증거 요구사항간의 만족성 확인	1 (기준치)
	적용 확인	1.3
	순응 확인	1.3
	부분결과 확인	1.3
	선택적 검증 확인	1.3
	분석결과 확인	1.3
	정확성 확인	1.3
	일관성 확인	1.3
	준수성 확인	1.3
	범위 확인	1.3
	수행 확인	1.3
결정 (독립적인 분석수행 필요)	구성 여부, 실현 여부 결정	2
	낮은 내성 결정	2.2
	중간내성 결정	5.8
	높은 내성 결정	9.6
	종속 관계 결정	2.3
시험	부분 시험	2.5
	시험 결과의 표본 시험	2.5
	시험 결과의 전체 시험	3
	독립 시험	4
	침투 시험	4
	추가적 침투 시험	4
반복 (재현)	설치 반복	1.5
	기타	1.5
취약성 분석	취약성 분석	4
문서의 스타일	준정형적 명세의 확인	0.3
	정형적 문서 스타일	0.5

표 5 정보보호 시스템의 평가 업무량 및 업무량의 상대적 비율

정보보호 제품 유형 / 보증수준(*)	OS	사용자 인증	접근통제	바이러스 방지	침입탐지
EAL1, D, E0, K1	111.7 (0.20)	63.7 (0.12)	111.7 (0.20)	223.4 (0.41)	135.2 (0.25)
EAL2, C1, E1, K2	346.0 (0.63)	263.0 (0.48)	307.9 (0.56)	231.8 (0.42)	214.5 (0.39)
EAL3, C2, E2, K3	**546.6 (1)**	360.8 (0.66)	470.1 (0.86)	256.9 (0.47)	240.5 (0.44)
EAL4, B1, E3, K4	932.1 (1.71)	419.4 (0.77)	689.8 (1.26)	-	-
EAL5, B2, E4, K5	1270 (2.32)	558.8 (1.02)	901.7 (1.65)	-	-
EAL6, B3, E5, K6	1532.4 (2.80)	735.6 (1.35)	-	-	-
EAL7, A, E6, K7	1691.3 (3.09)	-	-	-	-

(*) 각각 CC, TCSEC, ITSEC, K-CC에서 상호대응하는 보증수준임

에서 고려하는 제품유형들만을 고려하였다. 보증수준별 도구 사용율의 산정과정도 산출물의 크기산정과 유사하며 본 논문에서는 생략한다[25].

표 5의 괄호 안의 숫자는 "EFFORT(OS, EAL3)"을 1로 정했을 때의 상대적인 업무량 비율을 보인다. 예컨대, EAL 4급(TCSEC에서 B1급에 해당) 접근통제제품의 평가 업무량은 EAL 3급(TCSEC에서 C2에 해당) OS보다 1.26배 평가 업무량이 많음을 의미한다.

4.5 기초 평가비 산정 및 정산

unit_cost (= COST(*i, j*) / EFFORT(*i, j*))를 산정하기 위해 이미 알려진 평가비 자료를 베이스 자료로 활용한다. 선진국의 평가기관의 평가비 자료는 대외비로 처리되므로 정확히 알 수는 없지만, 본 연구에서는 입수한 정보를 통해 OS제품의 EAL3등급의 적정한 기초 평가 원가는 약 9만$임을 알 수 있었다[25].

즉, EFFORT(OS, EAL3)를 9만$이라면, unit_cost는 164.7$(=9만$/546.6)이 되며 표 8의 각 제품유형별 및 보증수준별 기초 평가비를 산정할 수 있다. 예컨대, 사용자 인증 제품의 EAL5에 대한 "기초 평가원가"는 12만 1153$(=164.7×735.6)이 된다. unit_cost값은 평가자의 임금, 평가도구 비용 등에 따라 매년 달라질 수 있지만 표 5에 나타난 제품유형 및 평가수준간의 비율은 평가기준의 함수이므로, 동일한 기준에 대해 항상 일정하다.

기초 평가비는 평균 수준의 평가환경(예; 평가자 능력, 소스코드 크기, 평가도구 수준 등)을 고려한 비용이므로, 22가지의 개발환경 속성을 응용하여 실제의 평가환경 속성 승수를 구한 후 평가비의 정산액을 구한다. 개발환경 속성에 대한 세부내용은 본 논문에서 생략한다[26].

4.6 도구의 사용

그림 6은 본 연구에서 개발 및 사용한 평가 업무량 및 평가비용 산정도구의 일부 쉬트를 보인다.

5. 분석 및 결론

5.1 소프트웨어 품질 평가 프로세스와 본 연구와의 관계

기존의 소프트웨어 품질 평가기준[1,2,3,4]은 모든 종류의 소프트웨어의 품질관리, 개발프로세스 및 제품의 평가를 위한 일반적인 지침과 평가절차를 제시하고 있다. 한편, CC는 그림 7처럼 기존의 국가별 정보보호 시스템 평가기준을 통합하고 소프트웨어 품질관리, 프로세스평가 및 제품의 품질평가 개념들을 통합한 정보보호 시스템 평가기준이다. 즉, 정보보호 시스템 평가기준은 제품유형이 정보보호 제품이며 평가대상 품질속성이 기능성과 보안성일 경우의 소프트웨어 평가기준에 해당한다.

정보보호 시스템의 평가철학, 방법론 및 기준은 기존의 소프트웨어 품질 평가기준의 한 인스턴스에 해당한다. 이 개념은 국제표준인 OSI 7층 프로토콜 표준(소프트웨어 품질 평가기준에 비유)과 TCP/IP프로토콜(CC에 비유)간의 관계에 비유할 수 있다.

본 연구에는 새로운 기준이나 평가 프로세스를 제시한 것이 아니며 기존의 기준(즉, CC)에 따라, 정보보호 시스템을 평가할 때의 평가 업무량과 비용을 EWBS를 이용해 산정하는 방법을 제시한 것이다. 본 방법은 소프트웨어 프로세스 품질 평가 및 소프트웨어 제품의 품질 평가시의 평가 업무량 산정에 그 개념을 활용할 수 있다. 그러나, 보안 관련 기능성 및 기능에 대한 보증성의 평가기준들이 매우 구체적으로 명시된 CC와는 달리, 소

[단계 1]보증수준별 평가업무량 산정 : *평가보증수준별 TOE 평가 업무량 산정표*

(1) 본 표에서는 보증수준별 평가업무량을 산정하는 것입니다.
(2) 현재의 자료는 CC2.0으로 세팅되어 있습니다. 평가기준이 바뀌면 노란색 부분의 값을 새로운 값으로 바꾸면 됩니다.
(3) 컴팩{}증 "제한{}"은 해당 패러리의 해당 제한{}의 페이지 수이며 "난이도"는 그의 평가 난이도입니다.

보증클래스	보증패밀리	EAL1			EAL2			EAL3			EAL4			EAL5			EAL6			EAL7		
		제품로 난이도	업무량		제품로 난이도	업무량		제품로 난이도	업무량		제품로 난이도	업무량		제품로 난이도	업무량		제품로 난이도	업무량		제품로 난이도	업무량	
형상관리	자동화										5.2	1	5.2	5.2	1	5.2	12	1	12	12	1	12
	능력	0.7	1	0.7	2.7	1	2.7	5.7	1	5.7	7.7	1	7.7	7.7	1	7.7	14.7	1	14.7	14.7	1	14.7
	범위							6.2	1	6.2	11.4	1	11.4	13.4	1	13.4	13.4	1	13.4	13.4	1	13.4
전달 및 운영	배포				2	1	2	2	1	2	6	1	6	6	1	6	6	1	6	6.7	1	6.7
	설치,생성,시동	4	3	12	4	3	12	4	3	12	4	3	12	4	3	12	4	3	12	4	3	12
개발	기능명세	11	3	33	11	3	33	11	3	33	17.7	3	53.1	17.7	3.3	58.4	17.7	3.3	58.4	17.7	3.5	62
	상위수준설계				12.2	3	36.6	22.2	3	66.6	22.2	3	66.6	22.2	3.3	73.3	24.6	3.3	81.2	24.6	3.5	86.1
	구현표현										21	3	63	47	3	141	48	3	144	48	3	144
	TSF 내부													7	3.3	23.1	16	3.3	52.8	19	4.8	91.2
	하위수준설계										26.9	3	80.7	26.9	3.3	88.8	27.9	3.3	92.1	27.9	3.5	97.7
	표현의임차성																					
	보안정책모델										12	1	12	18	1.5	27	18	1.5	27	19	1.5	28.5
지침문서	관리자설명서	15.3	1	15.3	15.3	1	15.3	15.3	1	15.3	15.3	1	15.3	15.3	1	15.3	15.3	1	15.3	15.3	1	15.3
	사용자설명서	15.7	1	15.7	15.7	1	15.7	15.7	1	15.7	15.7	1	15.7	15.7	1	15.7	15.7	1	15.7	15.7	1	15.7
생명주기	개발보안							8	2.3	18.4	8	2.3	18.4	8	2.3	18.4	13.2	2.3	30.4	13.2	2.3	30.4
	결함개선																					
	생명주기정의										2	1	2	5	1	5	5	1	5	8	1	8
	도구및기법										8.2	1	8.2	8.2	2.3	18.9	8.2	2.3	18.9	8.2	2.3	18.9
	범위				3	1	3	12	1	12	12	1	12	12	1	12	22	1	22	22	1	22
	깊이							3	1	3	3	1	3	5	1	5	5	1	5	7	1	7

그림 6 보증수준별 평가 업무량 쉬트의 예

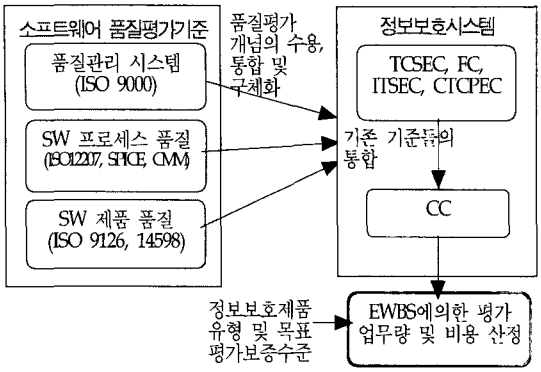


그림 7 본 연구와 소프트웨어 품질 평가기준 및 정보보호 시스템 평가기준간의 관계

프트웨어 품질 평가기준들은 평가대상 속성 및 척도의 정의[2]와 평가절차에 대한 일반적인 지침[3]으로 구성되어있으므로, 본 방법을 이용하기 위해서는 기존의 소프트웨어 품질평가 기준들을 CC와 같은 정도로 구체화 및 세분화 해야한다.

소프트웨어 제품의 평가시, 미리 정의된 평가모듈(Evaluation Module: EM)을 수정하여 사용하면 평가업무(평가요구사항 설정, 평가 명세화, 평가설계 및 평가수행)를 원활히 할 수 있다[3]. 즉, 평가자는 EM을 이용하므로써, 새로운 EM의 개발, 기존의 EM의 사용, 기존의 EM의 재사용 및 EM을 표준화할 수 있다. 정보보호시스템의 평가기준은 '정보보호 시스템의 기능성 및 보안성 평가용 EM'으로 간주할 수 있다.

정보보호 시스템의 평가시에도 미리 정의된 PP를 활용하고 있다. PP는 EM과는 달리 정보보호 제품 유형(예; OS, 사용자 인증, 접근통제 등)별로 평가대상물의 보안 환경, 보안 목적 및 보안 기능 요구사항들을 표준화한 것으로서, 정보보호 시스템의 개발자와 평가자는 이를 이용하여 간단히 보안목표 명세서(ST)를 개발할 수 있게 하고 있다. 즉, EM은 평가대상 품질특성별로 평가에 필요한 평가척도, 평가방법, 측정방법(도구 포함) 등을 재사용할 수 있게 한 것이며, PP는 정보보호 제품 유형별로 보안기능 요구사항들을 미리 정의하여 재사용할 수 있게 한 것이다.

5.2 본 연구의 의의와 향후 연구과제

본 연구는 다음과 같은 의의를 갖는다.

첫째, 본 연구는 "원가 회계학"적 접근방법이 아니라, 정보보호 시스템 및 소프트웨어 평가분야의 영역지식을 이용하여 평가 업무량 및 평가원가를 계산하였다. 특히, 소프트웨어의 개발 및 평가, 정보시스템 컨설팅 등과 같은 지식서비스 부문에서는 이러한 접근방법이 필수적이다. 따라서, 본 접근방법은 회계학에서의 원가계산 방법에 추가할 수 있을 것이다.

둘째, 기존의 소프트웨어 개발비 산정 방법들을 정보보호 시스템의 평가 업무량 산정시에 응용하였다. 즉, EWBS를 통해 평가기준을 단위 평가기준 및 단위 평가업무로 분해하는 방법, 각 단위 평가업무에 필요한 산출물의 크기를 산정하는 방법(베타분포를 이용해 산정시의 불확실성을 고려함), 단위 평가업무에 대한 평가의 난이도 산정 및 평가도구 사용을 산정 등은 소프트웨어 개발비 산정에서도 이용되는 방법들이다.

셋째, 평가기준이 주어졌을 때의 평가 업무량 및 평가비의 산정방법과 지원도구를 제시하였다. 평가기준은 평가업무에서의 요구사항 명세에 해당되므로, 평가 업무량은 오직 평가기준의 함수이며 평가환경은 평가비의 정산시에 실질 평가비를 구하기 위해 별도로 고려한다.

넷째, 영국의 정보보호 시스템 평가 비용은 평가대상물이 OS일 때의 비용을 1이라 할 때, DB는 1.5배, 방화벽은 0.6배 및 PC용 시스템은 0.4배로 알려져 있으며, 본 연구 결과에서는 OS를 1이라 할 때 방화벽은 0.8배이며 PC용 시스템은 0.47배로 나타났다. 또한, ITSEC을 평가기준으로 하는 영국에서 E1급을 1이라 할 때, E2급은 2배, E3급은 2.88배 및 E4급은 3.2배로 평가 비용이 든다. CC와 K-CC를 평가기준으로 한 본 연구의 결과에서는 EAL2급(E1급에 대응)을 1이라 할 때, EAL3(E2급에 대응)은 1.58배, EAL4(E3급에 대응)는 2.71배, EAL5(E4급에 대응)는 3.68배로 나타났다. 따라서, 본 연구 결과는 선진국에서의 보증수준별 및 정보보호제품 유형별 평가 비용과 근접함을 알 수 있다.

다섯째, 본 연구에 산정한 정보보호 시스템 평가기준 CC에 대한 보증수준별 및 제품유형별 평가 업무량의 상대적 비율과 평가비 산정 결과는, 국내·외 정보보호 시스템의 평가비 산정시에 활용할 수 있다.

본 연구에서는 기초 자료가 부족한 상태였으므로, 평가업무별 난이도의 산정과 산출물의 크기 예측시 주관적인 요소가 많으므로, 평가 비용상의 오차가 클 수 있다. 그러나, 국내·외적으로 정보보호 시스템을 포함한 각종 평가 경험과 결과가 축적되고 이를 고려한다면, 좀 더 실제적이며 오차가 적은 평가 비용을 산정할 수 있을 것이다. 이를 위한 평가 비용 및 평가 기간에 관련된 자료의 수집, 관리 및 분석 시스템이 마련되어야 하며, 난이도의 과학적이고 객관적인 산정을 위해 기존의 의사결정 이론들을 적용하는 연구를 향후의 연구과제로 남기고 있다. 또한, 기존의 소프트웨어 품질평가 기준과

정보보호 시스템의 평가기준에 대한 비교연구를 향후 연구과제로 남기고 있다.

참 고 문 헌

[1] S. L. Pfleeger, Software Engineering Theory and Practice, Prentice-Hall, Ch. 11, 1998.

[2] ISO/IEC 9126, "Information Technology - Software Quality Characteristics and Metrics - Part 1~3.

[3] ISO/IEC 14598, "Information Technology - Software Product Evaluation - Part 1~6.

[4] 양해술, 황석형, 정문재, "소프트웨어 제품 평가를 위한 ISO 14598-3의 적용방법", 99'춘계 한국정보처리학회 학술발표 논문집, 제 6권 1호, pp. 407~410.

[5] B. W. Boehm, Software Engineering Economics, Prentice-Hall, 1981.

[6] B. Boehm, et. al, "Cost Models for Furture Software Lifecycle Processes, Annals of Software Engineering Special Volume on Software Process and Production Measurement," http://sunset.usc.edu/ COCOMO-II/ cocomo.html#conferences, 1995.

[7] S. Chulani, "Incorporating Baysian Analysis to Improve the Accuracy of COCOMO II and Its Quality Model Extension," Univ. of Southern California, 박사학위 논문, http://sunset.usc.edu/ COCOMO-II/ cocomo. html#conferences, 1998.2.

[8] 西澤 脩, "정보처리비의 원가계산 방식", 와세다상학 358호, 1994. 2.

[9] "한국 소프트웨어사업 대가의 기준", 정보통신부고시 제 1998-4호, 1998.

[10] CCEB, "Common Criteria for Information Technology Security Evaluation(CC)", Version 2.0, CCIB-97/082, http://csrc.ncsl.gov, Dec 19, 1998.5.

[11] European Communication, "Information Security Evaluation Criteria(ITSEC)," Ver. 1.2, http://www.itsec.gov.uk, June 1991.

[12] DoD, "Department of Defense Trusted Computer System Evaluation Criteria (TCSEC)," Dec. 1985.

[13] "TPEP Procedure," http://www.radium.ncsc.mil, June 1996.

[14] "국내외 정보보호 시스템 가이드", 한국정보보호센터, 1998.11.

[15] CCEB, "Common Evaluation Methodology for Information Technology Security," Part 1(CEM-97/07), Part 2 (Version 1.0, CEM-99/045), http://csrc.ncsl.gov.

[16] "정보보호 시스템 평가기준(안) 0.7," 정보보호 시스템 평가기준 워크숍, 한국정보보호센터, 1998. 11. 26.

[17] "정보통신망 침입차단시스템 평가기준", 정보통신부고시 1998-19호, 한국정보보호센터, 1998.2.

[18] "엔지니어링사업 대가기준", 과학기술처 공고 제 97-28호, http://www.most.go.kr/announce/notify/6.html, 1997. 7.31.

[19] "Labeled Security PP," Version 1.0, ISSO, NSA, http://csrc.nist.gov/cc/, Sept. 1998.

[20] "Controlled Access PP," Version 1.b, ISSO, NSA, http://csrc.ncsl.gov/cc/, Sept. 1998.

[21] "U. S. Government Application-level Firewall PP for Low-risk Environment," Version 1.a, NIST, NSA, http://csrc.nist.gov/cc, Aug. 1998.

[22] "U. S. Government Traffic-filter Firewall PP for Low-risk Environment," Version 1.a, NIST, NSA, http://csrc.nist.gov/cc/, Aug. 1998.

[23] Role-based Access Control PP Version 1.0, NIST, http://csrc.nist.gov/cc/, July 1998.

[24] Information Technology Security Evaluation Manual(ITSEM), Commission of the European Communities, http://www.itsec.gov.uk, 1993.

[25] 이강수, "정보보호 시스템 평가수수료 산정방안 연구", 한국정보보호센터 연구보고서, 98-11, 1998.

[26] 장수진, 이강수, "소프트웨어 평가비 정산모델", 소프트웨어 공학연구회지, 한국정보처리학회, 2권 2호, 한국정보처리학회, pp. 19~28, 1999.

부록 A. 보증수준별 산출물 크기 산정 결과의 일부

보증 클래스	보증 패밀리	보증수준별 산출물 크기						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
형상 관리	자동화	-	-	-	5.2	5.2	12	12
	능력	0.7	2.7	5.7	7.5	7.7	14.7	14.7
	범위	-	-	6.2	11.4	13.4	13.4	13.4
중략								
개발	개발기능 명세	11	11	11	17.7	17.7	17.7	17.7
	상위수준 명세	-	12.2	22.2	22.2	22.2	24.6	24.6
	구현 표현	-	-	-	dsi ① (=21)	DSI+3 ② (=47)	DSI+3 ③ (=48)	DSI+3 ④ (=48)
중략								
지침 문서	관리자 설명서	15.3	15.3	15.3	15.3	15.3	15.3	15.3
	사용자 설명서	15.7	15.7	15.7	15.7	15.7	15.7	15.7
중략								
취약성	비밀채널 분석	-	-	-	-	17.2	20.2	20.2
중 략								
합계(반올림)		**56.7**	**130**	**193**	**294**	**361**	**422**	434

(주) ① "소스코드의 일부 크기"이며, K-CC 0.7에서 운영체제의 K4등급의 세부기능 요구사항 수가 126개이며, 이 값의 1/6을 취함(근거: 제출된 소스코드를 페이지로 환산하기 어려우며 소스코드 분석기를 사용하므로, 산출물의 양은 그리 많지 않게 산정함)
②~④ : K4등급의 세부 기능 요구사항수가 각각 141, 144, 144이므로 이의 1/3만을 취한 값에 3을 각각 더함

부록 B. 형상관리(CM) 보고서의 크기 산정과정의 일부

장	세부항목 (문서크기 중앙값)	문서크기				평가보증수준(EAL)						
		m	*a*	*b*	μ	1	2	3	4	5	6	7
1. 버전번호	- 평가대상물(TOE)에 대한 참조(TOE의 각 버전에 고유할 것) (0.2) - TOE의 참조용 레이블 (0.3)	0.5	1	1	0.7	O	O	O	O	O	O	O
2. 형상목록	- TOE를 구성하는 형상항목 (0.5) ... 중략 ...	2	2	2	2		O	O	O	O	O	O
3. CM계획	- CM시스템 사용 방법 (2) - CM시스템이 CM계획에따라 운영된다는 증거 (2)	4	3	5	3			O	O	O	O	O
	- CM시스템에서 사용하는 자동화된 도구 (1) - CM시스템에서 자동화된 도구 사용방법 (3)	4	3	5	3				O	O	O	O
4.CM시스템	- TOE구현 표현, 설계 문서, 시험 문서, 사용자 문서, 관리자 문서 및 형상관리 문서의 추적기능 (2) .... 중략...	6	4	9	6.2			O	O	O	O	O
	- TOE구현에 오직 인가된 변경만이 일어나도록 하는 자동화된 수단 (2) ...중략...	5	3	8	5.2				O	O	O	O
	- 개발자 도구 및 관련 정보 추적기능 (2)	2	1	3	2					O	O	O
	- TOE구현과 **다른모든형상항목**에 오직 인가된 변경만이 일어나도록 하는 자동화된 수단 (3) ...중략 ...	12	10	14	12						O	O
5. CM 인수계획	- 변경되거나 새로 생성된 형상항목을 TOE의 일부로 받아들일 때 사용한 절차 (2)	2	1	3	2				O	O	O	O
6. 통합절차	- CM시스템을 TOE 생산과정에 적용하는 방법 (2) ... 중략....	4	3	5	4						O	O
보증수준별 문서크기		μ				0.7	2.7	11.9	22.1	24.1	40.1	40.1
		a				1	3	10	17	18	31	31
		b				1	3	17	33	36	55	55

(주) a : 최선의 예측크기, b : 최악의 예측크기, m : 중간 예측크기, μ: 평균(=(a + 4m + b)/6)

부록 C 보증수준별 업무의 난이도 산정결과 일부

클래스	보증 패밀리	내용	보증수준별 난이도						
			EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
형상 관리	ACM_AUT	자동화	-	-	-	1	1	1	1
	ACM_CAP	능력	1	1	1	1	1	1	1
	ACM_SCP	범위	-	-	1	1	1	1	1
전 달 및 운영	ADO_DEL	배포	-	1	1	1	1	1	1
	ADO_IGS	설치, 생성, 시동	결정(2) 3	결정(2) 3	결정(2) 3	결정(2) 3	결정(2) 3	결정(2) 3	결정(2) 3
	증략								
개발	ADV_LLD	하위수준 설계	-	-	-	결정(2) 3	결정(2),준정형(0.3) 3.3	결정(2), 준정형(0.3) 3.3	결정(2),정형(0.5) 3.5
	ADV_RCR	표현의 일치성	1	1	1	1	1	준정형(0.3) 1.3	결정(2), 정형(0.5) 3.5
	ADV_SPM	보안정책 모델	-	-	-	1	정형(0.5) 1.5	정형(0.5) 1.5	정형(0.5) 1.5
지침 문서	AGD_ADM	관리자 설명서	1	1	1	1	1	1	1
	AGD_USR	사용자 설명서	1	1	1	1	1	1	1
	증략								
취약성	AVA_CCA	비밀채널 분석	-	-	-	-	분석결과확인(1.3), 선택적검증(3) 5.3	분석결과확인(1.3), 선택적검증(3) 5.3	분석결과확인(1.3), 선택적검증(3) 5.3
	증략								
	AVA_VLA	취약성 분석	-	침투시험(4) 5	침투시험(4) 5	침투시험(4), 취약성분석(4), 추가침투시험(4), 낮은내성결정(2.2) 15.2	침투시험(4), 취약성분석(4), 추가침투시험(4), 중간내성결정(5.8) 18.8	침투시험(4), 취약성분석(4), 추가침투시험(4), 중간내성결정(5.8) 18.8	침투시험(4), 취약성분석(4), 추가침투시험(4), 높은내성결정(9.6) 22.6

(주) "산출물과 증거 요구사항간의 만족성 확인" 업무는 모든 항목에 공통적으로 포함됨(난이도=1)

유 형 준

1998년 한남대학교 컴퓨터공학과 학사. 1998년 ~ 현재 한남대학교 컴퓨터공학과 석사과정. 관심분야는 소프트웨어 공학, 워크플로우모델링, 정보보호시스템 평가체계, 전자상거래 정보보호(특히, 키 관리, 스마트카드) 등임

장 수 진

1985년 충남대학교 계산통계학과 학사. 1991년 충남대학교 계산통계학과 석사. 1994년 ~ 현재 대전보건대학 전산정보처리과 교수. 1998년 ~ 현재 한남대학교 컴퓨터공학과 박사과정. 관심분야는 소프트웨어공학, 정보보호, 전자상거래

고 정 호

1997년 한남대학교 컴퓨터공학과 학사. 1999년 한남대학교 컴퓨터공학과 석사. 1999년 ~ 현재 한남대학교 컴퓨터공학과 박사과정. 관심분야는 소프트웨어 컴포넌트, 정보보호, 전자상거래

안 선 숙

1992년 서원대학교 회계학과 학사. 1995년 한남대학교 경영학과 석사. 1999년 한남대학교 회계학과 박사수료. 1996년 ~ 현재 한남대학교 회계학과 강사. 관심분야는 관리회계, 원가계산(특히, 소프트웨어 원가계산)

이 강 수

1981년 홍익대학교 컴퓨터공학과 학사. 1983년 서울대학교 계산통계학과 석사. 1989년 서울대학교 계산통계학과 박사. 1985년 ~ 1986년 국립대전산업대학교 전임강사. 1987년 ~ 현재 한남대학교 컴퓨터공학과 교수. 1992년 미국 일리노이대학교 교환교수. 1995년 한국전자통신연구원 초빙연구원. 관심분야는 소프트웨어 공학, 패트리넷응용, 워크플로우 모델링, 모니터링 시스템, 정보보호시스템 평가체계 등임

정 홍 진

1976년 중앙대학교 경영학과 학사. 1978년 서울대학교 경영학과 석사. 1987년 중앙대학교 경영학과 박사. 1983 ~ 1984년 미국 U of North Carolina 객원교수. 1996년 ~ 1997년 일본 와세다대학 상학부 객원교수. 1979년 ~ 현재 한남대학교 회계학과 교수. 관심분야는 관리회계, 원가계산