情報保護學會論文誌
第17卷 第4號, 2007. 8

CC 2.3과 CC 3.1의 보증수준별 상대적 평가업무량 배율 추정

고 갑 승,† 김 영 수‡, 이 강 수‡
한남대학교

Estimation of relative evaluation effort ratios for each EALs in CC 2.3 and CC 3.1

Kab-seung Kou,† Young-Soo Kim, Gang-soo Lee‡
Hannam University

요 약

공통기준(CC) 평가체계에서 평가신청인과 평가자는 평가프로젝트를 계약할 때 정보보호시스템의 평가비용과 기간을 산정해야한다. 본 논문에서는 2003년과 2005년에 수행한 연구 결과들을 분석하였으며, 연구 결과의 일부분을 활용하여, CC 2.3과 CC 3.1의 평가보증수준(EAL1~EAL7)간의 상대적 평가업무량 배율을 실험조사적으로 산정했다. 또한, 각 보증 컴포넌트에 대해 '개발자요구사항', 조정된 '증거요구사항', '평가자요구사항'으로부터 배율을 산정하였고, 특히, 2003년에 KISA 평가 자료로부터 구한 평가자요구사항별 업무량배율을 사용했다. 본 연구의 결과는 새로운 CC 3.1 평가체계에서 특정한 EAL과 제품유형에 대한 평가비용과 기간을 예측해야하는 평가신청인과 평가프로젝트 관리자에게 유용할 것이다.

ABSTRACT

In Common Criteria evaluation scheme, sponsor and evaluator should estimate evaluation cost and duration of IT security system evaluation in contracting the evaluation project. In this paper, We analyzed study result that achieve at 2003 and 2005, and utilized part of study result. And we empirically estimate relative evaluation effort ratios among evaluation assurance levels (EAL1~EAL7) in CC v2.3 and CC v3.1. Also, we estimate the ratios from 'developer action elements', adjusted 'content and presentation of evidence elements', and 'evaluator action elements' for each assurance component. We, especially, use ratio of amount of effort for each 'evaluator action elements', that was obtained from real evaluators in KISA in 2003. Our result will useful for TOE sponsor as well as evaluation project manager who should estimate evaluation cost and duration for a specific EAL and type of TOE, in a new CC v3.1 based evaluation scheme.

Keywords : *CC(Common Criteria), 평가업무량, 평가수수료*

접수일: 2007년 4월 25일 ; 채택일: 2007년 6월 18일
* 본 연구는 2007년도 2단계 두뇌한국(BK)21 사업과 산업자원부 지역혁신센터사업인 민군겸용보안공학연구센터 지원으로 수행되었음.
† 주저자, kabseung@se.hannam.ac.kr
‡ 교신저자, gslee@eve.hannam.ac.kr

Ⅰ. 서 론

정보화 사회에서 정보는 가치를 가진 자산으로 간주함에 따라, 정보 자산에 대한 보호가 필요해졌고 다양한 정보보증(information assurance) 제도, 방법 및 표준 등

이 운영되고 있다[1]. 기존의 정보보증 제도들은 다음과 같이 분류 할 수 있다.

- 생명주기별 : 설계/구현, 통합/시험, 전개/전이, 운용
- 타겟 그룹별 (유형별) : HW벤더, SW벤더, 네트워크 사용자, 서버 제공자, 컨텐츠 제공자, 기업(사용자)
- 타겟 그룹별 (조직내 역할별) : 경영자, 프로젝트관리, IT 보안담당자, IT 관리자, 관리자, 감사자
- 보증대상물(TOE) 수준별 : 암호모듈, 제품, 응용시스템, 합성형 시스템
- 개발 및 운용환경별 : 프로세스, 조직 환경, IT 운용환경
- 표준별: 평가기준, 평가방법론 및 평가체계

예를 들면, 현재 정보보호시스템(또는 제품)의 국제공통기준(Common Criteria)인 CC v3.1(ISO/IEC 15408)은 '생명주기별' 측면에서 설계/구현, 통합/시험, 전개/전이에 적용되고, '타겟 그룹별(유형별)' 측면에서 HW벤더와 SW벤더에 적용되며, '타겟 그룹별(조직 내 역할별)' 측면에서 프로젝트관리, IT 보안담당자 및 IT 관리자에 적용된다. 또한, '평가대상물(TOE) 수준' 측면에서 제품에 적용되고 '개발 및 운용환경' 측면에서는 해당이 없으며, '표준별' 측면에서 평가기준은 CC v3.1, 평가방법론은 CEM v3.1이며, 평가체계는 미국의 경우 NIAP(The National Information Assurance Partnership)의 CCEVS(Common Criteria Evaluation and Validation Scheme)이다[2, 3, 4].

미국의 FIPS 140-2를 표준으로 하는 '암호모듈' 수준의 평가체계인 CMVP(Cryptographic Module Validation Program)와 '운영 중인 시스템' 수준의 보안관리 인증체계의 표준인 ISO/IEC 17799 (또는, 영국 BS 7799)와 함께, CC는 국제적으로 인정되는 정보보호 '제품' 수준의 평가 기준이다[5, 6].

2007년 3월 현재 CC v3.1이 공식 버전이며 11개의 인증서 발행국과 12개의 인증서 소비국이 CCRA (Common Criteria Recognition Arrangement)에 협정하여 평가 결과를 상호인정하고 있다. 그동안 국가별 평가체계를 통해 수백 종의 정보보호 제품이 CC로 평가되어 '평가제품 목록'(EPL)에 등재되어 있다.

CC 평가체계의 주요역할인 '소비자', '개발자' 및 '평가자(또는 전문가)'중 개발자와 평가자는 평가대상물의 평가기간과 평가비용에 관심이 있으며, 특히, CC 평가를 위해서 평가신청인(sponsor)과 평가기관 간에 평가계약을 할 때, 평가대상물의 유형(예: 제품 유형별 보호프로파일, 제품의 보안목표명세서), 목표로 하는 보증수준(예: EAL1 ~ EAL7) 및 평가환경(예: 평가 컨설팅 수준, 평가기관의 능력 등)에 따라 평가비용과 평가기간을 결정해야한다.

이와 같은 배경에서 본 논문에서는 기존의 기준인 CC v2.3과 새롭게 지정된 공식기준인 CC v3.1의 보증수준별 상대적 평가업무량의 배율을 예측하는 방법을 제시한다. 본 연구는 본 연구팀이 2003년과 2005년에 수행한 연구결과를 일부 활용하며, 본 논문의 결과는 CC v3.1 기반의 정보보호 제품의 평가를 위한 평가비용과 기간의 산정에 이용될 수 있을 것이다.

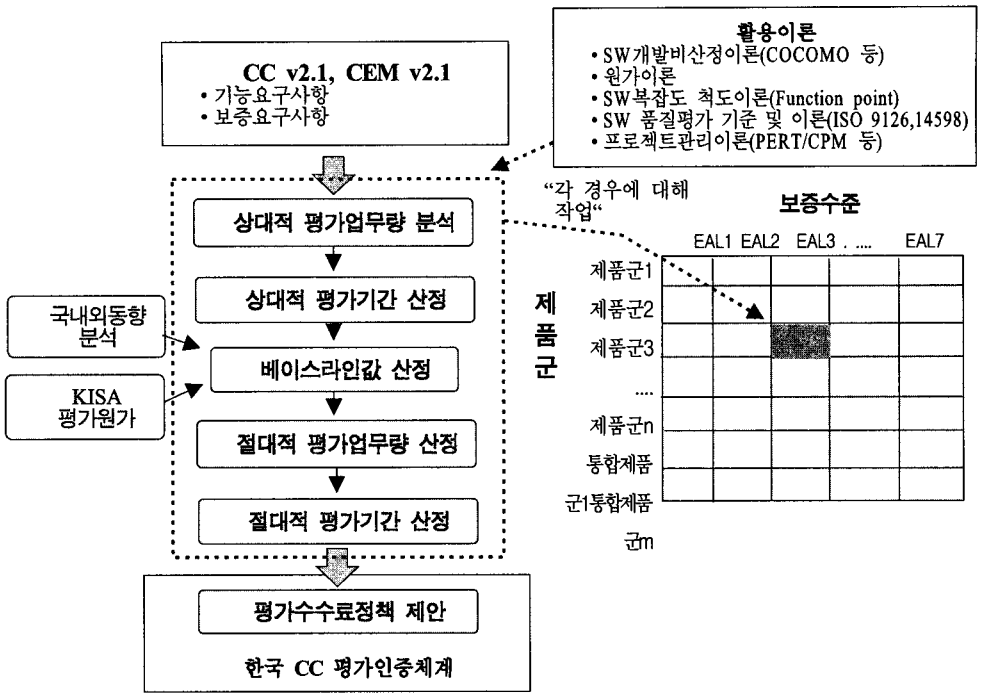
본 논문의 2장에서는 과거의 CC v2.1과 한국 평가기준(침입차단 및 탐지시스템 평가기준)을 기반으로 한 기존의 연구결과와 외국의 동향을 정리한다. 3장에서는 CC v2.3과 CC v3.1의 보증수준별 상대적 평가업무량 배율의 산정방법과 결과를 제시하며, 4장에서는 분석과 평가결과를 보이며 5장에서 결론을 맺는다.

Ⅱ. 기존의 연구결과

1980년대 중반부터 미국의 TCSEC(Trusted Computer System Evaluation Criteria)을 기준으로 한 낮은 보안수준의 국가용 평가 체계인 TPEP(Trusted Product Evaluation Program), 상용 제품의 평가체계인 TTAP (Trust Technology Assessment Program)체계, 1990년대 유럽의 ITSEC(Information Technology Security Evaluation Criteria)을 기준으로 한 정보보호제품 평가체계 및 2000년대 이후 각국에서는 CC를 기반으로 하여 많은 평가가 실시되었다. 그러나 보증 수준별 (TCSEC의 경우 A1, B3, B2, B1, C2, C1, D 등급, ITSEC의 경우 E1~E6등급) 및 제품유형별 평가업무량 (비용과 기간)에 관한 정보는 다음과 같은 이유 때문에 잘 알려져 있지 않다.

- 제품의 생산 원가처럼, 평가기관의 수준과 역량에 관련된 문제이므로, 일반적으로 대외비로 취급한다.
- 평가는 변호사 업무와 같이 컨설팅 형태의 활동이므로, 평가신청인과 평가자간의 당사자 계약에 의해 평가기간과 비용을 정한 후 사후 정산한다.
- 평가환경(평가대상물의 복잡성, 평가기관의 평가도구, 평가자의 능력, 평가자에 대한 협조)에 차이가 많다.

예를 들면, X라는 평가기관에서 DBMS 유형의 제품을 EAL4로 평가하는데 1년이 소요되었고 2억 5천만원을 평가기관에 지불했다는 정도의 단편적인 정보만



〔그림 1〕 2003년 연구의 접근방법

존재하고 있다. 외국에서는 지금까지 보증수준별 상대적 평가업무량에 대해 연구한 사례는 부족하지만, 우리나라는 CCRA가입에 따라 '민간 평가기관' 제도를 도입하고 평가비용을 현실화하기 위한 기초 연구로서 KISA의 지원으로 2건(2003년 및 2005년)의 위탁연구를 수행되었다〔7, 8, 9〕.

2.1. 2003년의 연구내용

2003년의 연구에서는 〔그림 1〕과 같은 방법을 통해 CC v2.1의 보증수준별 및 제품유형별 평가업무량을 산정하였다〔7, 8〕.

2.1.1. 상대적 평가업무량 분석

첫째, KISA 평가팀의 평가실무자로부터 "평가자 요구사항"(평가자 행동) 요소별 난이도 가중치를 설문조사하고(예: 평가자 요구사항중 "표본검사"는 0.54이며 "취약성분석"은 6.11이다)(〔표 1〕 참조). 여기서, 난이도 가중치는 평가업무량에 비례한다고 가정한다. 이를 이용하여, EAL1~EAL7 및 PP, ST별 평가업무량을 산정하였다. 산정결과는 〔표 2〕의 행과 같다. 둘째, 제품유형별 평가업무량을 산정하기위해, 2003년 8월 중에 인터넷에 올라있는 33종의 PP와 67종의 ST를 분석하여 산정하였다. 산정결과 〔표 2〕의 열과 같다. 셋째, 보증수준 및 제품유형별 평가업무량의 배율을 구하기 위해, 보증수준별 평가업무량과 제품유형별 평가업무량을 카테이션 프로덕트하였다. 〔표 2〕는 결과를 보인다. 여기서, DB제품유형의 EAL1을 1로 정했다.

2.1.2. 상대적 평가기간 산정

평가업무량은 평가기간×평가자수(Man-Month)이며, 평가자수를 3명으로 고정하면, 평가업무량은 평가기간에 비례한다. 따라서, 보증수준 및 제품유형별 평가업무량 배율을 평가기간의 배율로 사용한다.

2.1.3. 베이스라인값 산정

KISA의 자료 및 외국의 실제 평가비용 및 기간정보를 수집하였으며, 다음과 같이 분석하였다.

- 평가팀의 인원: CC평가의 특수성과 기존의 평가가 팀에 관한 정보를 토대로 평가팀은 3명 정도(고급, 중급, 초급기술자)로 구성한다.

〔표 1〕 정보보호시스템의 평가난이도 가중치

설문항목 \ 설문결과		난이도 가중치 (최대·최소를 제외한 평균값)
검사(check)	1. 표본검사	0.54
	2. 모든검사	0.78
확인(confirm) - 충족여부의 확인	3. 제출물과 증거요구사항 간의 만족성 확인(기준업무)	1.00
	4. 적용 확인	1.41
	5. 순응 확인	1.46
	6. 부분결과 확인	1.34
	7. 선택적 검증 확인	1.40
	8. 분석 결과 확인	1.41
	9. 정확성 확인	1.68
	10. 일관성 확인	1.63
	11. 표준 준수성 확인	1.47
	12. 범위 확인	1.33
	13. 수행 확인	1.38
결정(determine) - 독립적인 분석수행 필요	14. 구성여부, 실현 여부 결정	2.15
	15. 낮은 내성 결정	2.61
	16. 중간 내성 결정	5.92
	17. 높은 내성 결정	9.71
	18. 종속 관계 결정	2.53
시험(test)	19. 부분 시험	2.35
	20. 시험 결과의 표본 시험	2.40
	21. 시험 결과의 전체 시험	5.24
	22. 독립 시험	4.97
	23. 침투 시험	5.45
	24. 추가적 침투 시험	5.26
설치반복 (재현)	25. 설치의 반복(재현)	1.48
	26. 기타	1.49
취약성 분석	27. 취약성 분석	6.11

〔표 2〕 CC v2.1 보증수준 및 제품유형별 평가업무량 배율

보증수준 및 평가업무량 배율 / 제품유형 및 평가업무량 배율		PP	EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7	평균
		0.48	1.00	1.39	1.62	2.15	2.39	2.69	2.80	1.81
DB	1.00	0.48	1.00	1.39	1.62	2.15	2.39	2.69	2.80	1.81
침입차단	0.92	0.44	0.92	1.28	1.49	1.98	2.20	2.47	2.58	1.67
VPN	1.88	0.90	1.88	2.61	3.05	4.04	4.49	5.06	5.26	3.41
네트워크	1.50	0.72	1.50	2.09	2.43	3.23	3.59	4.04	4.2	2.73
OS	1.71	0.82	1.71	2.38	2.77	3.68	4.09	4.60	4.79	3.11
스마트카드	1.68	0.81	1.68	2.34	2.72	3.61	4.02	4.52	4.70	3.05
접근통제	1.65	0.79	1.65	2.29	2.67	3.55	3.94	4.44	4.62	2.99
키복구	1.24	0.60	1.24	1.72	2.01	2.67	2.96	3.34	3.47	2.25
침입탐지	0.93	0.45	0.93	1.29	1.51	2.00	2.22	2.50	2.60	1.69
기타	1.25	0.60	1.25	1.74	2.03	2.69	2.99	3.36	3.50	2.27
평균	1.38	0.66	1.38	1.91	2.23	2.96	3.29	3.70	3.85	2.50

• 평가기간: 평가기간에 관한 정보를 바탕으로 '침입차단 제품유형의 EAL4의 평가기간은 10개월'로 정하였다. 따라서 〔표 2〕의 (EAL4, 침입차단) 요소의 배율 값이 1.98이며 이 값을 10개월로 본다.

• 평가비용: 평가비용에 관한 정보를 바탕으로 '침입차단시스템의 EAL4의 평가비용은 2억 2,160 (17만7천

〔표 3〕 2005년 연구의 주요결과 (ST평가를 포함시킴)

연구결과	항목	EAL1 (K1)	EAL2 (K2)	EAL3 (K3)	EAL4 (K4)
KISA의 실제 평가기간 및 평가원가	평가기간(일)	129	177	231	345
	평가비용(원)	1억 274만	1억 4,000.8만	1억 8,332만	2억 7,296.5만
	등급별 비율	1	1.36	1.78	2.66
CC v2.3에 기반한 표준 평가기간	표준평가기간(일)	60	99	116	187
	등급별 비율	1	1.6	1.9	3.1

〔표 4〕 복잡도 계수의 정의

복잡도 등급	복잡도 계수	분류기준	평가제품
낮음	0.8	상대적으로 작은 규모의 단순한 IT 제품	스마트가드 판독기, OS보안시스템, 생체인식, 무선랜, SW 암호모듈, 프린터
보통	1	상대적으로 중간규모의 복잡성을 갖는 IT제품	PC보안, 침입차단, 침입탐지, 가상사설망, 라우터, 스위치, HW암호모듈, 일반 응용 프로그램
높음	1.2	상대적으로 큰 규모이며 복잡한 IT 제품	스마트카드 OS, 컴퓨터 OS, IC칩

$)만 원'으로 정하였다.

따라서 〔표 2〕의 (EAL4, 침입차단) 요소의 배율 값은 1.98이며 이 값을 2억 2,160만 원으로 본다.

2.1.4. 절대적 평가업무량 산정 및 평가기간 산정

〔표 2〕에 베이스라인 값을 고려하여 제품유형별 보증수준별 절대적 평가업무량을 구하였다. 예를 들면, 스마트카드의 EAL3 (〔표 2〕에서 배율 값이 2.72임)의 평가비용은 3억 442만 원(=2.72×2억2,160만 원/1.98)이며, 평가기간은 13.7개월(=2.72×10개월/1.98)이다.

2.2. 2005년의 연구내용

2.2.1. 관련자료 조사 및 KISA 평가원가 계산

2005년의 연구에서는 KISA 평가팀의 2000년~2002년간의 실제 평가원가 계산을 실시하였다. 이 기간에는 CC 평가가 거의 이루어지지 않았고, 침입차단과 침입탐지시스템평가 기준에 의한 K등급평가를 실시하였으므로 CC의 평가원가는 아니지만, K등급과 EAL간에는 매우 연관성이 높으므로 이 결과를 CC 평가업무량의 계산에 이용하였다〔9〕.

또한, KISA, 호주, 미국, 독일의 평가기관으로부터 입수한 평가기간 관련 정보(예: 보증클래스별 평가기간, 제품유형별 보안기능수)를 수집하며 평가 비용 및 평가기간 산정시의 베이스라인으로 사용하였다. 〔표 3〕에는 KISA의 실제평가기간 및 평가원가를 보인다.

2.2.2. 클래스 단위별 평가일수 산정

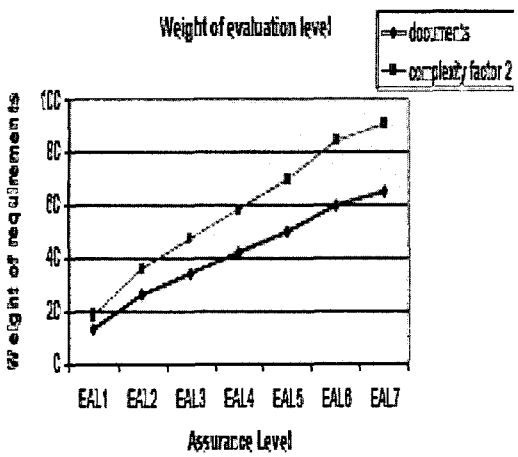
관련 자료로 부터 '작업단위' 개수를 기준으로 하여 보증수준별 평가업무량 비율을 구했다. 따라서 EAL1 : EAL2 : EAL3 : EAL4 = 1 : 1.5 : 1.7 : 2.4이다.

2.2.3. 단위업무별 표준 평가기간 산정

보증수준별 평가업무량의 배율과 관련 자료로부터 〔표 3〕과 같이 보증수준별 표준 평가기간을 구했다. 따라서, EAL4의 표준 평가기간은 187일이다.

2.2.4. 실제 평가기간 산정

보안기능수, 제품별 복잡도 계수를 고려하여 다음과



〔그림 2〕 보증수준별 문서량과 복잡도의 증가

같이 산정한다.

평가기간 = (보안기능수/30) × 표준평가기간 × 복잡도계수

- '보안기능수': 평가대상물의 평균 보안기능수는 30개라고 가정함
- '복잡도계수': 〔표 4〕에 따라 정함

2.2.5. 인건비 산정

한국소프트웨어산업협회의 'SW기술자 노임단가 기준'을 적용하며 다음과 같이 산정한다〔10〕.

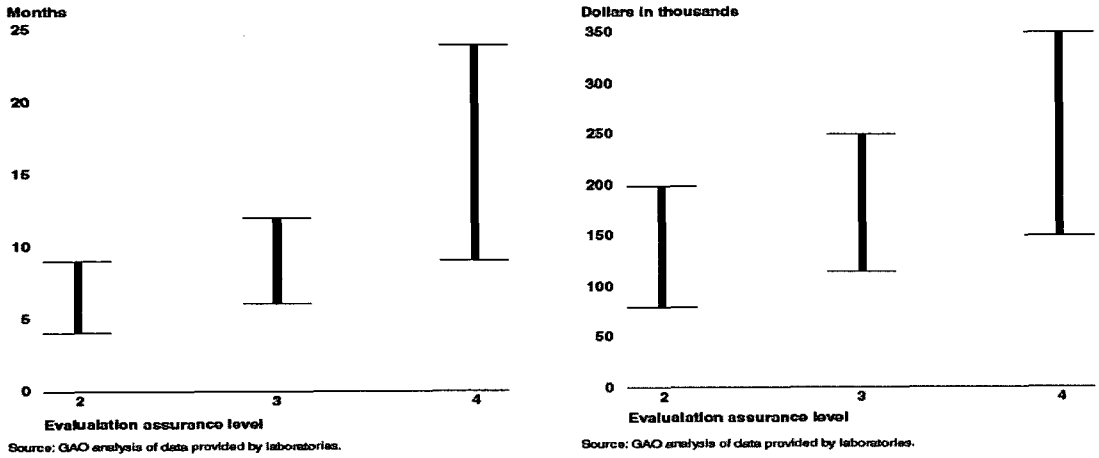
- 인건비 = ∑{평가기간(일) × 투입인력별단가}
- 도구사용비 = 투입인력의 인건비의 7% 반영
- 제경비 = 투입인력의 인건비 대비 110% 반영 (정통부의 '소프트웨어사업대가의기준', 과기부의 '엔지니어링사업대가기준' 적용) 〔11, 12〕

2.3. CC 평가 관련 정보

CC 평가비용과 기간은 원칙적으로 평가자와 평가기관간의 계약에 의해 결정되며, 평가대상제품의 특징과 평가가관의 환경에 따라 편차가 큰 것으로 알려져 있다. 〔그림 2〕는 2006년 자료이며 보증수준별 문서량과 복잡도의 증가를 보인다〔13〕. 〔그림 3〕은 보증수준별 평가기간과 비용에 관한 미국 GAO의 2006년 조사보고서의 내용을 보인다〔14〕. 또한, 독일의 CC 인증기관인 Federal Office for Information Security (BSI)에서는 〔표 5〕와 같이 보증수준별 등록수수료를 고시하고 있다〔15〕. 이 수수료는 우리나라의 평가수수료와는 다른 것이며 인증관리 비용이다〔16〕.

2.4. 소프트웨어 개발비 및 시험비 산정

B. Boehm의 COCOMO 모델과 Function Point 모델을 이용하여 개발된 우리나라의 "소프트웨어사업대가기준"에서는 SW개발비, SW 유지보수 및 재개발비, 시스템 운용환경 구축비(설계비, 환경조성비), 데이터베이스 구축비 및 정보전략계획(ISP) 수립비만을 산정하며, 이를 CC 평가비 산정에 적용하기에는 무리가 있다〔11,



〔그림 3〕 미국 GAO의 조사결과 (2006년, 미국 평가기관)

〔표 5〕 독일 인증체계에서 보증수준별 인증관리 수수료 (단위: 유로)

제품유형 \ EAL	EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
단순형 제품 (예: 스마트카드리더)	1,200 (150만원)	2,300	3,670	4,670 (584만원)	6,210	8,290	10,920 (1,365만원)
중간형 제품 (예: PC보안, 스마트카드 응용 SW, 일반응용 SW)	1,700	3,080	5,250	6,790	8,840	11,670	15,050
복잡형 제품 (예: OS, 스마트카드 HW와 OS, firewalls)	2,780 (347만5천)	4,130	6,500	9,040 (1,130만원)	12,170	16,050	20,420 (2,553만)

17, 18〕. CC 평가업무는 제출물의 확인과 검증, 독립시험, 침투시험, 취약성 분석, 설치의 반복 등과 같은 업무로 구성되므로, 기존의 개발비 산정기준을 적용하기 어렵다.

한편, 각종 공인 시험기관(시험소)에서는 건설, 환경, 화학 등의 분야에서 주로 하드웨어적인시험을 실시하고 시험원가 계산을 통해 산정하고 미리 고시한 시험비용을 부과한다. 이 경우 시험비용이 정해져있으며 시험자의 공수(man-day)별 인건비도 정해져있다. 예를 들면, 마이크로소프트사의 시험비용은 미리 정해져 있으며 'platform'시험($400), 'designed for' 시험($600~$11,000), 'certified for' 시험($1,000$~$30,000$), 'retired' 시험($25,000~$20,000)이다.(https://partner.microsoft.com/global/)

또한, Cisco에서는 보안시험 비용으로 $5,400~$7,750을 받는다(http://www.keylabs.com/cisco/csec/fees.html).

2.5. 기존 연구의 문제점

2003년의 연구는 CC v2.1을 대상으로한 것이며 현재의 CC v3.1과 CC v2.3에 적용할 수 없다. 2005년의 연구는 KISA 평가팀의 2000년 ~ 2002년간의 실제 평가환경을 고려한 것이며, 당시에는 CC 평가가 거의 이루어지지 않았고 침입차단과 침입탐지시스템평가 기준에의한 평가가 이루어졌다.

특히, Gorge의 연구결과는 〔그림 2〕만 나타나있을 뿐 세부사항이 없고 독일의 인증관리 수수료인 〔표 5〕의 내용은 평가비용과는 다르다. 현재의 사실상의 기준인 CC v2.3과 공식 기준인 CC v3.1에 대한 보증수준별 상대적 평가업무량에 대한 연구가 이루어지지 못했다.

CC v3.1에서 보안기능은 거의 변동이 없으나 보증기준이 대폭 변경되었는데, 평가복잡도의 관점에서 어느 정도 변경되었는지 알 필요가 있다. 예를 들면, CC v2.3에서 EAL2와 EAL3간의 평가복잡도 차이는 CC v3.1에서 EAL2와 EAL3간의 차이와 얼마나 다른지 알 필요가 있다. 이 자료는 평가기관에서 평가프로젝트 관리를 위해 매우중요하다. 끝으로, CC v3.1에 있는 합성제품의 보증수준별 상대적 업무량에 대한 연구결과는 전무하다.

Ⅲ. CC v2.3과 v3.1의 보증수준별 상대적 업무량 산정

3.1. 산정방법

CC의 각 보증요구사항 컴포넌트는 '개발자요구사항'(developer action elements)', '증거요구사항'(content and presentation of evidence elements), '평가자요구사항'(evaluator action elements) 요소로 구성되어 있다〔2〕. TOE의 개발자는 '개발자요구사항' 요소대로 TOE를 개발하며, 평가신청인은 '증거 요구사항' 요소대로 제출물을 제출하며, 평가자는 '평가자 요구사항'대로 평가를 실시한다.

모든 보증요구사항 컴포넌트의 평가자 요구사항중 "평가자는 제공된 정보가 모든 증거요구사항을 만족하는지 확인해야 한다."(The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.)는 모든 요소에 공통적이며(이를 '평가자 공통요구사항'이라 칭한다.), 어떤 컴포넌트는 추가적인 평가자요구사항 요소들이 있다. 보증 컴포넌트의 '평가자 공통요구사항'은 평가 신청자가 제출한 '증거요구사항'의 요소별 제출물에 대해 일관성 등을 확인(confirm)만 하면 되므로, 업무량은 많지 않다. 또한, '평가자 공통 요구사항'의 업무량은 '증거요구사항' 요소의 수와 요소별 내용(예: 전체, 일부,

정형, 반정형 등)에 비례한다. 특히, 본 연구에서는 어떤 보증에 대한 절대적인 평가업무량을 산정하는 것이 아니라, 보증수준별 상대적 평가업무량의 배율을 산정하는 것이므로, 보증 컴포넌트의 '평가자 공통요구사항'의 업무량을 산정할 때, '증거요구사항' 요소의 개수와 수준만을 고려하였다.

3.1.1. 보증컴포넌트별 증거요구사항 개수 파악과 조정

CC v2.3과 CC v3.1에서 보증수준이 증가함(보증 패밀리 내에서 컴포넌트의 번호가 증가)에 따라, '증거요구사항'의 요소개수는 증가하지 않았지만 요소문장의 내용만 변경된 경우도 있다. 예를 들면, 하위 보증수준에서 '부분'이라는 단어가 상위 보증수준에서 '전체'로 변경되고 '비정형적'은 '반정형적' 또는 '정형적'으로 변경된다. 따라서, 다음 규칙을 통해 증거요구사항의 요소 개수를 조정하였다.

보증패밀리 AF내의 보증컴포넌트 i의 (이를 AF.i 로 표시)의 '증거요구사항'의 요소문장을 AF.i.Ck (k = 1 , ... , #AF.i.C)라하고 증거요구사항 요소의 개수를 #AF.i.C 로 표시하고, 조정된 증거요구사항 요소의 개수를 #AF.i.C* 라 하자.

그러면 다음조건을 만족해야한다.

#AF.i.C ≤ #AF.i+1.C (i=1, ..., n)

#AF.i.C* ≤ #AF.i+1.C* (i=1, ..., n)

#AF.i.C ≤ #AF.i.C* (i=1, ..., n)

이를 위해, 다음 계산식을 적용한다.

① #AF.1.C* = #AF.1.C

② #AF.i.C* = #AF.i.C + 달라진문장수 × 0.5 (i = 2, ..., n)
(상위 컴포넌트의 요소개수는 하위 컴포넌트의 요소개수와 같지만 요소문장의 내용 다를 때. 예를 들면, '일부'가 '전부'로 변경, '비정형'이 '반정형'으로 변경 등, 달라진 문장당 0.5씩 증가 시킴)

③ if #AF.i.C > #AF.i+1.C then #AF.1+1.C* = #AF.i.C* + 1 (CC v3.1의 ADV_FSP에서 이 문제 발생)

예를 들면, CC v3.1의 ADV_FSP 패밀리의 6개의 보증 컴포넌트에 대한 증거요구사항 개수의 조정사례는 〔표 6〕과 같다.

※ ADV_FSP.4에서, #ADV_FSP.4.C = 6이므로 앞 컴포넌트보다 문장수가 줄었으며(CC v3.1의 오류로 판단됨) 규칙 ③에따라, #ADV_FSP.4.C* = 9+1 = 10이 된다.

3.1.2. 보증 컴포넌트별 업무량 배율산정

CC에서 각 보증 컴포넌트의 '평가자요구사항'에는 모든 컴포넌트에 공통 요소인 '평가자 공통요구사항' 이외에도 다양한 평가자요구사항 요소가 있다. (예를 들면, '독립시험을 해야 한다' 등) 이런, 추가적인 평가자 요구사항 요소들은 평가자가 별도로 수행해야하는 업무이며, 요소의 종류에 따라 그 업무량(또는, 난이도)이 달라야한다.

본 논문의 2장에서 보인바와 같이 2003년의 연구에서 각 평가자요구사항 요소중 '평가자 공통요구사항'의

〔표 6〕 ADV_FSP 패밀리의 증거요구사항 개수의 조정 사례

항목 \ 컴포넌트	ADV_FSP.1	ADV_FSP.2	ADV_FSP.3	ADV_FSP.4	ADV_FSP.5	ADV_FSP.6
문장수 (#AF.i.C)	4	6	7	6	9	10
추가된문장수		2	1	-1	3	1
강화된 문장내용		'complete', 'all', 'describe'	'complete', 'all', 'describe', 'summarise'	'all'	'complete', 'all', 'describe', 'summarise', 'all', 'semiformal'	'complete', 'all', 'describe', 'summarise', 'all', 'semiformal', 'formal'
조정된 문장수 (#AF.i.C*)	4	7.7 = 6 + 3×0.5	9 = 7 + 4×0.5	10 = 9+1	11 = 9 + 6×0.5 = 11	13.5 = 10 + 7×0.5

〔표 7〕 AVA_VAN 패밀리의 평가자 요구사항의 평가업무량 배율산정 예 (괄호안의 숫자는 요소의 배율)

보증 컴포넌트 / 항목	ADA_VAN.1	ADA_VAN.2	ADA_VAN.3	ADA_VAN.4	ADA_VAN.5
평가자요구사항 요소	- confirm [1]	- confirm [1]	- confirm [1]	- confirm [1]	- confirm [1]
	- perform (공개소스 search)[0.78]	- perform (공개소스 search)[0.78]	- perform (공개소스 search)[0.78]	- perform (공개소스 search)[0.78]	- perform (공개소스 search)[0.78]
	- 침투시험 (파악된 취약성에 대해 Basic 공격잠재성)[4.45]	- 침투시험 (파악된 취약성에대해, Basic 공격잠재성)[4.45]	- 침투시험 (파악된 취약성에 대해, Enhanced-Basic 공격잠재성)[5.45]	- 침투시험 (파악된 취약성에 대해, Moderate 공격잠재성)[6.45]	- 침투시험 (파악된 취약성에 대해, High공격잠재성)[7.45]
		- perform (독립 취약성분석)[6.11]	- perform(독립 취약성분석, 구현표현 추가)[7.11]	- perform(독립 및 방법론적 취약성분석, 구현표현 추가)[7.11]	- perform(독립 및 방법론적 취약성분석, 구현표현 추가)[7.11]
업무량 합계	6.23	12.34	14.34	15.34	16.34

〔표 8〕 CC v2.3과 CC v3.1의 보증수준별 평가업무량 배율

항목 \ 보증수준		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
패밀리 개수	CC v2.3	15	21	25	31	34	34	34
	CC v3.1	13	19	22	24	25	27	27
개발자요구사항 요소 개수	CC v2.3	20	31	35	46	52	54	58
	CC v3.1	17	31	35	39	42	45	50
증거 요구사항 요소 개수	CC v2.3	68	93	107	140	156	178	181
	CC v3.1	49	84	98	108	113	125	130
조정된 증거요구사항 요소개수	CC v2.3	68	93	109	143	162	187	193
	CC v3.1	49	86	103	116.5	123	138.5	146
평가자 요구사항 전체 업무량	CC v2.3	91.9	128.59	149.63	203.51	231.25	267	279.41
	CC v3.1	64.81	113.47	131.88	147.38	158.5	177.65	190.61
평가자 요구사항 전체 업무량의 상대적 배율	CC v2.3	1	1.4	1.63	2.21	2.52	2.9	3.04
	CC v3.1	1	1.75	2.03	2.27	2.45	2.74	2.93

업무량을 1이라 정했을때 다른 요소의 상대적 업무량의 배율을 KISA에 근무하는 실제 평가자로부터 설문으로 통해 구했다. 본 연구에서는 2003년의 연구결과인 〔표 1〕을 사용한다.

〔표 7〕은 AVA_VAN 패밀리의 평가자 요구사항의 평가업무량 배율산정의 예를 보인다. 〔표 1〕을 기준으로 하여 '독립취약성분석'은 6.11, '구현표현추가'는 7.11로 가정하였고, 특히, '침투시험'의 경우, 수준이 정해지지 않은 경우를 5.45로하고 basic 수준을 4.45, enhanced-basic 수준을 5.45, moderate 수준을 6.45, high 수준을 7.45로 가정하였다.

3.1.3. 보증 컴포넌트별 평가업무량 산정

앞에서 구한 조정된 증거요구사항 개수 (#AF.i.C*)와 보증 컴포넌트별 업무량 배율산정 결과(@AF.i.C)를 이용하여 보증 컴포넌트별 평가업무량을 산정한다. 보증 컴포넌트 AF.i의 평가업무량을 &AF.i 라 하면,

&AF.i = #AF.i.C* + @AF.i.C - 1

(여기서, - 1을 한 이유는 '평가자 공통요구사항'이 중복 카운트되기 때문이다.)

〔표 9〕 보증수준별 및 제품별 평가업무량 배율

제품유형별 평가업무량 배율 \ 보증수준 및 평가업무량 배율			EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7	평균
		CC v2.3	1	1.40	1.63	2.21	2.52	2.9	3.04	1.71
		CC v3.1	1	1.75	2.03	2.27	2.45	2.74	2.93	2.03
DB	1.00	CC v2.3	1.00	1.40	1.63	2.21	2.52	2.90	3.04	1.59
		CC v3.1	1.00	1.75	2.03	2.27	2.45	2.74	2.93	2.03
침입차단	0.92	CC v2.3	0.92	1.29	1.50	2.03	2.32	2.67	2.80	1.49
		CC v3.1	0.92	1.61	1.87	2.09	2.25	2.52	2.70	1.92
VPN	1.88	CC v2.3	1.88	2.63	3.06	4.15	4.70	5.45	5.72	2.65
		CC v3.1	1.88	3.29	3.82	4.27	4.61	5.15	5.51	3.27
네트워크	1.50	CC v2.3	1.50	2.10	2.45	3.32	3.78	4.35	4.56	2.19
		CC v3.1	1.50	2.63	3.05	3.41	3.68	4.11	4.40	2.74
OS	1.71	CC v2.3	1.71	2.39	2.79	3.78	4.31	4.96	5.20	2.45
		CC v3.1	1.71	2.99	3.47	3.83	4.19	4.69	5.01	3.02
스마트카드	1.68	CC v2.3	1.68	2.35	2.74	3.71	4.23	4.87	5.11	2.41
		CC v3.1	1.68	2.94	3.41	3.81	4.12	4.60	4.92	2.99
접근통제	1.65	CC v2.3	1.65	2.31	2.69	3.65	4.16	4.79	5.02	2.38
		CC v3.1	1.65	2.89	3.35	3.75	4.04	4.52	4.83	2.95
키복구	1.24	CC v2.3	1.24	1.74	2.02	2.74	3.12	3.60	3.77	1.88
		CC v3.1	1.24	2.17	2.52	2.81	3.04	3.40	3.63	2.37
침입탐지	0.93	CC v2.3	0.93	1.30	1.52	2.06	2.34	2.70	2.83	1.51
		CC v3.1	0.93	1.63	1.89	2.11	2.28	2.55	2.72	1.93
기타	1.25	CC v2.3	1.25	1.75	2.04	2.76	3.15	3.63	3.80	1.89
		CC v3.1	1.25	2.19	2.54	2.84	3.06	3.43	3.66	2.38
평균	1.38	CC v2.3	1.24	1.99	2.37	2.93	3.30	3.78	4.06	
		CC v3.1	1.24	1.99	2.37	2.93	3.30	3.78	4.06	

3.1.4. 보증수준별 평가업무량 배율 산정

보증 컴포넌트별 평가업무량 산정 결과와 CC의 제 3부 보증요구사항에 정의된 보증수준별 보증요구사항 정의표로부터, CC v2.3과 CC v3.1의 EAL1부터 EAL7까지의 평가업무량을 구한다.

3.1.5. CC v3.1의 합성제품 보증수준(CAP)별 평가업무량 배율산정

합성제품의 평가업무량 산정을 위해 CC v3.1의 ACO 클래스에서 정의한 3가지 보증수준인 CAP-A, CAP-B, CAP-C에 대해 앞의 (1)~(4) 과정을 반복 적용한다. CAP-A, CAP-B, CAP-C는 각각 EAL2, EAL3, EAL4에 대응한다〔19〕.

- CAP-A (구조적 합성)
- CAP-B (방법론적 합성)
- CAP-C (방법론적 합성, 시험 및 검토)

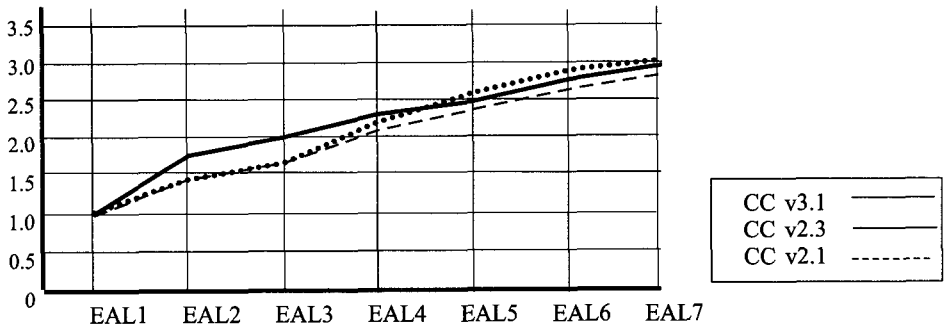
3.2. 산정결과

3.1절에서 제시한 방법을 적용하여 〔표 8〕의 CC

〔표 10〕 합성형 정보보호제품의 보증수준별 평가업무량 배율

항목 \ 보증수준	CAP-A	CAP-B	CAP-C
패밀리 개수	15	16	16
개발자요구사항 요소 개수	21	23	23
증거요구사항 요소 개수	55	68	71
조정된 증거요구사항 요소 개수	55.5	69	72
평가자 요구사항 전체 업무량	75.86	95.47	99.47
평가자 요구사항 전체 업무량의 상대적 배율	1	1.26	1.31

〔그림 4〕 CC에서 보증수준에 따른 평가업무량 배율의 변화



〔표 11〕 기존 연구와의 비교

기준 및 연구결과 \ EAL		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
본 연구	CC v3.1	1	1.75	2.03	2.27	2.45	2.74	2.93
	CC v2.3	1	1.4	1.63	2.21	2.52	2.9	3.04
	CC v2.3 (ST평가 불포함시)	1	2.24	2.95	4.76	5.7	6.91	7.32
2003년 연구 (CC v2.1)		1	1.39	1.62	2.15	2.39	2.69	2.80
2005년 연구	KISA 실제 평가원가 (CC기준아님)	1	1.36	1.78	2.66	-	-	-
	KISA 예측 평가기간	1	1.65	1.93	3.11	-	-	-
KISA 수수료	최초평가 비율	1	1.26	1.63	2.16	3.06	3.85	4.74
	재평가 비율	1	1.72	2.58	3.30	4.16	4.88	5.74
	K등급 재평가 비율	1	2	3	4	5	6	7
독일 BSI 체계 인증관리 수수료	단순제품	1	1.92	3.06	3.89	5.18	6.91	9.1
	중간제품	1	1.81	3.09	3.99	5.2	6.86	8.85
	복잡제품	1	1.49	2.34	3.25	4.38	5.77	7.35

v2.3과 CC v3.1의 보증수준별 평가업무량 배율을 구하였다. 특히, CC v3.1에는 ST평가업무(AST 클래스)가 모든 EAL에 공통으로 포함되어있으므로 CC v2.3에서도 AST 클래스를 모든 EAL에 포함시켰다. 또한, 합성형 정보보호제품의 보증수준별 평가업무량 배율은 〔표 10〕에서 보인다.

본 논문의 2장에서 제시한 2003년의 연구결과중 제품유형별 상대적 평가업무량 배율을 적용하면 〔표 9〕와 같다〔7, 8〕.

Ⅳ. 분석 및 평가

〔표 11〕과 〔그림 4〕에서 보인바와 같이 CC v2.1 (2003년 연구결과)에서 보증수준 간 평가업무량 배율은 매우 유사하다. 이는 두 버전간의 차이가 거의 없기 때문이다. 그러나 CC v3.1은 EAL2와 EAL3 에서 CC v2.3과 차이를 보이고 있다. 따라서 CC v2.3은 EAL1에서 EAL2로 바뀔 때 1.4배이지만 CC v3.1.은 1.75배이며, EAL 3으로 바뀔때는 각각 1.63배(CC v2.3에서)와 2.03배(CC v3.1에서)로 증가한다. 특히, CC v2.3은 EAL2로 증가할 때는, 0.4가 증가했지만 EAL3에서는 EAL2보다 0.23증가했다. CC v3.1의 경우, EAL2로 증가할 때는, 0.75가 증가했지만, EAL3에서는 EAL2보다 0.28 증가했다. 3장에서 제시한 방법을 CC v2.3과 CC v3.1에 대해 동일하게 적용하였으므로, 이 결과는 신뢰할만하다. 결론적으로, CC v3.1에서는 낮은 수준(EAL2와 EAL3)에서 CC v2.3보다 평가업무량이 많다. 따라서 기존의 CC v2.3에 의한 평가비용보다 많은 평가비용이 소요될 것으로 예측된다.

그러나, 합성형 시스템의 3가지 보증수준 간에는 수

〔표 12〕 베이스라인을 고려했을 평가비용의 산정 예

보증수준 / CC	EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
CC v3.1	1억1,013만	1억9,796만	2억2,963만	2억5,192만	2억7,715만	3억995만	3억3145만
CC v2.3	1억1,331만	1억5,837만	1억8,439만	2억5,000만	2억8,507만	3억2,805만	3억4,389만

준간의 평가업무량의 배율은 크지 않다. 따라서 CAP-A : CAP-B : CAP-C = 1 : 1.26 : 1.31로 산정되었다.

각 보증수준별 상대적 평가업무량(평가기간 또는 평가비용)의 배율을 연구한 결과는 2장에서 설명하였지만 본 연구는 다른 접근방법을 사용하고 있다. 특히, KISA의 보증수준별 평가수수료의 배율 값이나 독일의 인증수수료의 배율 값은 그 근거가 공개되어있지 않다. 예를 들면, 독일 BSI에서 단순제품의 EAL7수준의 수수료가 EAL1보다 9.1배이지만, 복잡 제품의 경우 7.35배인지 알 수 없다.

만일 CC v2.3에서 EAL4의 평가비용이 〔그림 3〕에 나타난 2006년 GAO의 조사결과로부터 25만$(2억 5,000만원. 이를 '베이스라인 값'이라 한다)으로 가정한다면, 각 보증수준별 평균 평가비용은 〔표 12〕와 같다. CC v2.3의 EAL2, EAL3 및 EAL4의 평가비용은 미국 GAO에서 조사한 평가비용(앞 절의 〔그림 3〕)과 유사하다.

한편, 보증수준별 평가기간도 이와 유사하게 산정할 수 있다. 특히, 대부분의 CC 평가기관에서 평가인원이 3명 정도로 고정되어 있으므로, 평가비용과 평가기간은 거의 비례한다. 〔그림 3〕에서 이런 현상을 볼 수 있다.

V. 결 론

본 연구의 주요결과는 다음과 같다.

CC v2.3과 CC v3.1에서 보증수준간의 상대적 평가업무량의 배율을 산정하였다. 이 결과는 향후 각 평가기관에서 CC v3.1기반의 평가 시에 평가기간과 평가비 산정에 이용할 수 있다.

보증 컴포넌트별 증거요구사항 요소 개수의 조정 방법을 사용하였다.

2003년의 보증 컴포넌트의 평가자요구사항 요소별 평가업무량 조사 결과를 CC v2.3과 CC v3.1에 적용하여 보증컴포넌트별 평가업무량을 산정하였다.

CC v3.1의 합성형 제품의 3가지 보증수준간의 상대적 평가업무량의 배율을 산정하였다.

보증수준별 평가비용 또는 평가기간에 관한 자료를 수집하고 분석하였다.

본 연구로부터 알려진 사항은 CC v3.1의 경우 낮은 보증수준에서 CC v2.3보다 평가업무량이 많으며(0.35 ~ 0.4), CC v2.3보다 좀 더 많은 평가비용이 소요될 것으로 예상된다.

1970년대 이후 소프트웨어 개발비용과 기간의 산정 방법과 기준은 잘 알려져 있으나, CC 평가업무와 같은 유형의 소프트웨어 시험의 비용과 기간에 관한 연구는 부족하다. 향후, 기존의 소프트웨어 개발비용 산정기술을 적용하여 CC기반의 평가비용의 산정에 이용하는 연구가 필요하다. 또한, 실제 평가기관으로부터 CC v3.1의 보증수준별 평가비율을 구하여 본 연구의 결과를 검증하는 일을 향후 연구과제로 남긴다.

참고문헌

〔1〕 ISO/IEC TR 15443, "Information technology - Security Techniques - A Framework for it Security Assurance", 2001.

〔2〕 Common Criteria for Information Technology Security Evaluation Part 1, 2, 3, Version 3.1, Revision 1, September 2006.

〔3〕 Common Criteria for Information Technology Security Evaluation - Evaluation methodology, Version 3.1, Revision 1, September 2006.

〔4〕 Common Criteria for Information Technology Security Evaluation Part 1, 2, 3, Version 2.3, August 2005.

〔5〕 FIPS 140-2, Security Requirements for Cryptographic Modules, May 2001. [http://csrc.nist.gov/cryptval/]

〔6〕 ISO/IEC 17799, Information technology - Security techniques - Code of practice for information security management, June 2005.

〔7〕 "공통평가기준 기반 평가기간 산정 방안 및 평

가수수료 정책 연구", 한국정보보호학회 (한남대학교), KISA연구보고서, 2003.11.

〔8〕 최상수, 최승, 이완석, 이강수, "CC기반에서 보증수준 및 제품유형을 동시에 고려한 평가업무량 모델", 정보보호학회논문지, 14권 1호, pp.25-34, 2004년 2월.

〔9〕 "평가수수료개선을 위한 수수료모델 타당성조사", 한영회계법인, KISA연구보고서, 2005.12.

〔10〕 "SW기술자 노임단가 기준", 한국소프트웨어산업협회, 2006.

[11] "소프트웨어사업대가의 기준", 정보통신부 공고, 제2005-22호 개정 (2006. 4. 27) http://www.sw.or.kr.

〔12〕 "엔지니어링사업대가기준", 과학기술부 공고, 2004.

〔13〕 F. Forge, "Ways to CC evaluation cost reduction - beyond CC V3", 7'th ICCC, Sep. 2006.

〔14〕 Information Assurance - National Partnership Offers Benefits, but faces considerable challenges, GAO-06-392, GAO, March 2006. http://www.gao.gov/new.items/d06392.pdf

〔15〕 Regulations on Ex-parte Costs on Official Acts of the Federal Office for Information Security (BSI Regulations on Ex-parte Costs - BSI-KostV), March 2005 http://www.bsi.bund.de/english/exparte_costs.pdf

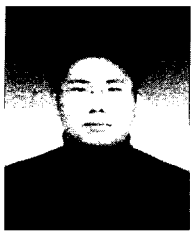
〔16〕 정보보호시스템 평가.인증인증가이드, KISA, 2006.12.

〔17〕 B. Boehm, et al., "Software Cost Estimation with COCOMO II", Prentice-Hall, 2000.

〔18〕 T. Jones, "Estimating Software Costs", McGraw-Hill, 1998.

〔19〕 Albert B. Jeng and Yu-Min Yu, "Analysis of the composition problems in CC v3.1 rev.1 with some suggested solutions", ICCC 2006, 스페인, 2006.9.

〈著者紹介〉



고 갑 승(Kab-Seung Kou) 정회원

2005년 2월 : 영동대학교 컴퓨터공학과 학사
2007년 2월 : 한남대학교 대학원 컴퓨터공학과 석사
2007년 3월~현재 : 한남대학교 대학원 컴퓨터공학과 박사과정
<관심분야> 소프트웨어공학, 보안공학, 정보보호 컨설팅 및 위험분석

김 영 수(Young-Soo Kim) 정회원

1989년 2월 : 전북대학교 학사
1992년 2월 : 경희대학교 대학원 석사
2003년 2월 : 국민대학교 대학원 정보관리학과 박사
2006년 3월~현재 : 한남대학교 컴퓨터공학과 연구교수
<관심분야> 전자상거래, 인터넷 응용, 분산정보시스템, 정보보안

이 강 수 (Gang-Soo Lee) 종신회원

1981년 2월 : 홍익대학교 전자계산학과 학사
1983년 2월 : 서울대학교 대학원 전산학과 석사
1989년 : 서울대학교 대학원 전산학과 박사
1985년~1987년 : 국립한밭대학교 전자계산학과 전임강사
1992년~1993년 : 미국일리노이대학교 객원교수
1995년 : 한국전자통신연구원 초빙연구원
1998년~1999년 : 한남대학교 멀티미디어학부장
1987년~현재 : 한남대학교 컴퓨터공학과 정교수
<관심분야> 소프트웨어공학, 병행시스템 모델링 및 분석, 보안공학, 정보보호시스템 평가, 멀티미디어교육 커리큘럼