情報保護學會論文誌
第14券 第1號, 2004. 2

CC기반에서 보증수준 및 제품유형을 동시에 고려한 평가업무량 모델*

최 상 수,[a)†] 최 승,[a)‡] 이 완 석,[b)] 이 강 수[a)]
한남대학교,[a)] 한국정보보호진흥원[b)]

An assurance level and product type based evaluation effort model for CC evaluation

Sang-Soo Choi,[a)†] Seung Choi,[a)‡] Wan-Suck Yi,[b)] Gang-Soo Lee[a)]
Hannam University,[a)] Korea Information Security Agency[b)]

요 약

CC(=ISO/IEC 15408)는 정보보호시스템의 국제표준이며 CC평가 및 인증체계에서는 평가기관을 운영하며 평가기관에서는 적정한 평가비 산정을 위한 근거가 필요하다. 본 논문에서는 특정한 평가기관의 환경이 아니라, CC기준과 기존의 PP 및 ST만을 바탕으로 하여, 제품유형별 및 보증수준별 평가업무량 모델을 제시하였으며, 평가실무자들의 경험, 보안기능의 사용율 개념 및 기능점수방법 등을 이용하였다. 본 결과는 CC평가환경에서 정보보호제품의 평가비 및 기간의 산정을 위한 기본자료로 활용될 수 있을 것이다.

ABSTRACT

Common Criteria(CC, ISO/IEC 15408) is an international standard for evaluation of Information Security Systems(ISS). There need a suitable evidence of estimation of evaluation cost in an evaluation facility under the CC-based evaluation and assurance scheme. In this paper, we propose an evaluation effort model, which is based not only on assurance-level but also on product-type of ISS, by means of real experience of real evaluators, use-ratio concept and the Function Point of security function. The model is based not on a real evaluation environment of evaluation facility, but on CC, public PPs and product specific STs. Our result might be used as a basic model for estimation of evaluation cost and time of ISS in an CC-based evaluation and assurance scheme.

Keywords: *Common Criteria, Assurance Level, Product Type, Evaluation Effort Model*

Ⅰ. 서 론

정보화사회에서 보안 및 프라이버시 문제와 같은 정보화의 역기능문제는 필연적이며, 정보보호기술은 정보화의 역기능을 예방, 방지, 발견 및 복구하기 위한 종합기술이다. 특히, 정보보호시스템 평가·인증체계는 정보화의 역기능문제를 다소 해결하며 정보보호시스템의 품질(특히, 보안성)을 평가하고 공인하는 것이다. 미국의 TCSEC과 FC, 유럽연합의 ITSEC, 카나다의 CTCPEC은 자국내 정보보호시스템의 평가기준이며, 국가마다 상이한 평가기준을 연동시키고

접수일: 2003년 9월 15일; 채택일: 2004년 1월 6일
* 본 연구는 2003년도 한국정보보호진흥원의 연구비지원으로 수행된 결과임 일부임.
† 주저자, gcss09@se.hannam.ac.kr
‡ 교신저자, schoi@se.hannam.ac.kr

평가결과를 상호인증하기 위해 제정된 사실상의 국제 기준은 CC(Common Criteria, ISO/IEC 15408)이다.[1~4]

CC를 포함한 정보보호시스템 평가·인증 체계에서 평가비와 평가기간은 평가대상물의 특성, 평가기관의 환경, 평가신청인의 협조여부에 따라 편차가 크며, 평가기관과 평가신청인간의 업무적 계약에 따른다고 명시되어있다.[5] 따라서, 평가기관은 평가계약을 위해 평가비용과 기간에 대한 근거의 제시가 필요하다.

이러한 배경에서, 본 논문에서는 CC 2.1 및 final interpretation[4] 기반의 정보보호시스템을 위한 적정한 평가비용 및 기간의 산정을 위해, CC와 PP(즉, 제품유형별 공통 보안요구사항명세서) 및 ST(특정제품의 보안요구사항명세서)를 분석하여, 제품유형별 및 보증수준별 평가업무량 모델을 개발한다.

CC는 정보보호시스템의 보안 및 보증요구사항명세서에 해당하며 구현사례도 부족하므로, 보안요구사항의 구현비용(즉, 개발비용)을 정확히 예측할 수는 없다. 또한, CC만을 통해 평가비를 산정한다는 것은 불가능하며 CC기반의 평가원가와 기간은 평가환경에 따라 차이가 크므로, 본 논문에서는 평가비 및 기간의 산정시에 다음과 같은 가정을 세웠다.

- 평가비용은 보증수준 및 제품유형에 상관관계가 있음
- 개발기간 및 비용(즉, 노력량)은 평가기간 및 비용(노력량)에 비례함
- 제품/보증수준별 상대적 노력량을 모델로 함
- ST 평가비용은 평가비용에 포함

본 논문의 접근방법인 상향식 배율산정법은, CC의 보증컴포넌트별 평가자행동의 난이도를 분석하여 보증수준별 상대적 평가업무량을 산정하고, 기존의 PP 및 ST의 보안기능요구사항들을 분석하여 보안기능의 사용율, 기능점수 및 기능컴포넌트간의 계층성을 이용하여 제품유형별 평가업무량을 구하고 이를 카테이션프로덕트하여 보증수준 및 제품유형별 상대적 평가업무량을 산정하는 것이며 2차원적인 평가업무량모델이다.

본 논문의 2장에서는 CC기반의 정보보호시스템의 기본개념을 소개하고, 3장에서는 CC의 보증수준별, 제품유형별 평가업무량 모델을 제시한다. 4장에서는 기존의 연구결과와의 차이를 제시하며 결론을 맺는다.

Ⅱ. CC기반의 정보보호시스템 평가방법

2.1 CC의 구성

CC는 그림 1과 같이 모든 정보보호시스템에서 필요로 하는 보안기능요구사항의 전체집합을 클래스-패밀리-컴포넌트-엘리먼트를 통해 계층적으로 분류되어 있다. 또한, 보안기능에 대하여 구현의 정확성에 대

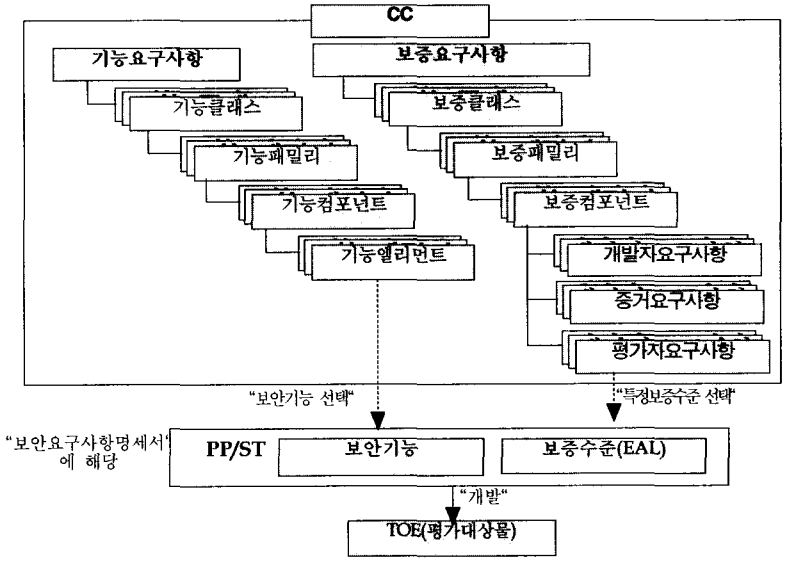


그림 1. CC의 구성과 사용의 개념

한 보증요구사항의 전체집합을 계층적으로 분류하였고 7단계의 보증수준별로 요구하는 보증요구사항(컴포넌트)을 정의하고 있다. 상위의 보증수준은 하위의 보안수준보다 완전하고, 엄격하며 정형적이므로, 보증수준간에는 완전성, 엄격성 및 정형성관계를 갖는다.[2.3]

정보보호시스템(TOE; Target of Evaluation, 평가대상물)의 제품유형에 따라 CC 보안기능요구사항의 일부를 선택하고 7수준의 보안수준 중 하나를 택하여 PP(protection profile) 또는 ST(security target)를 구성한다.

2.2 PP, ST 및 TOE간의 관계

PP는 제품유형별 공통보안요구사항명세서이며 특정한 제품유형의 운영에 대한 보안환경(가정, 보안정책, 위협문장을 포함) 보안목적, 보안요구사항(보안기능 요구사항 및 보안보증 요구사항)으로 구성된다. 보안요구사항에서의 보안기능은 CC의 보안기능 요구사항집합의 부분집합이며, 보안보증은 보안보증 요구사항집합의 부분집합이다. 일반적으로 PP는 사용자(PP 개발자)가 원하는 요구사항을 포함하여 개발하며 별도의 PP평가와 인증이 요구된다.

ST는 특정한 정보보호제품(즉, 평가대상물, TOE)의 보안요구사항명세서이다. 해당 제품유형의 PP가 존재할 경우, 기존의 PP에 개발환경을 부가하여 사용할 수 있으며 이 경우 "PP준수선언"이 필요하다.[6] ST는 TOE의 보안요구사항명세서에 해당하므로, ST도 TOE와 함께 평가 및 인증한다.

예컨대, 그림 2에서 PP들 및 ST(또는 TOE)들 사이에는 보안기능이 중복될 수 있다. ST3(TOE3)의 보안기능은 PP3의 보안기능을 사용하므로 ST3

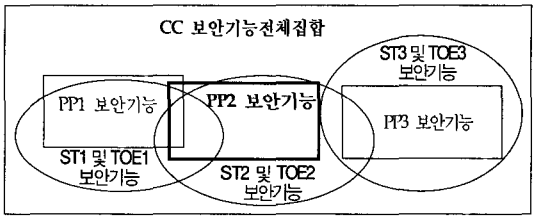


그림 2. CC의 보안기능전체집합과 PP, ST 및 TOE별 보안기능간의 포함관계

은 PP3을 그대로 사용할 수 있다. 이때, ST3내에는 PP3에 대한 준수선언이 필요하다. PP, ST 및 TOE의 개발 및 평가절차는 그림 3에서 보인다.

Ⅲ. CC 평가업무량 모델

3.1 보증수준별 평가업무량

CC는 보안기능요구사항 집합과 보증요구사항 집합으로 구성되며 표 1은 보증요구사항 집합에 나타난 보증수준별 업무수를 보인다. 표 1은 단순히 업무를 표현한 항목의 수 일 뿐이며, 각 항목을 수행하기 위한 업무량(또는 난이도)은 서로 다르므로, 표 1을 보증수준별 평가업무량의 배율로 볼 수는 없다.

본 논문에서는 CC의 보증수준별 평가업무량을 산정하기 위해, CC 보증요구사항의 각 컴포넌트에 정의된 "평가자행동" 및 "근거요구사항"(즉, 개발자의 자체평가 업무 및 평가자에게 제출해야할 전달물 내용 및 수준을 명시한 문장)을 고려하였다. "평가자행동"에서 사용하는 "단어"(예: 검사, 확인, 결정, 시험 등)는 평가업무량 및 난이도에 관련되므로, 본 논문에서는 2003년 5월에 평가경험이 있는 한국정보보호진흥원의 직원 20명으로부터 설문·조사하여 표 2

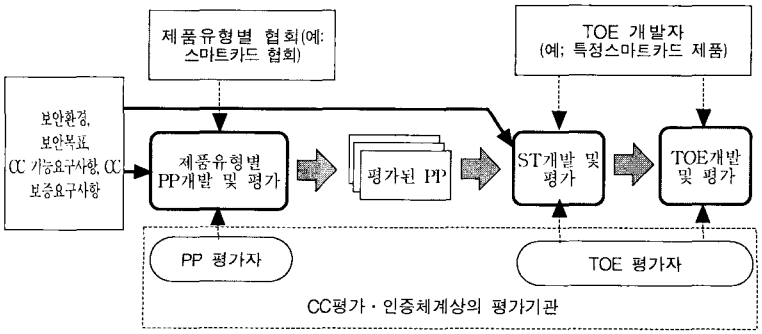


그림 3. CC체계하에서 PP, ST 및 TOE의 개발 및 평가절차

표 1. CC에서의 보증수준별 업무수

항목 \ 보증수준		PP 평가	ST 평가(*)	보증수준						
				EAL1 (베이스라인)	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
CC 패밀리수		6	8	7	13	17	23	23	25	25
개발자 요구사항수		9	11	7	18	22	33	33	40	45
증거 요구사항수		32	41	23	47	63	94	90	132	135
평가자 요구사항수		14	45	10	20	27	39	39	44	47
CC Work unit	개수	32	41	23	47	63	94	108	132	135
	추가업무수	-	-	-	-	2	7	15	20	28
	추가업무수	8	11	3	7	10	16	20	21	22
	합계	40	52	26	54	75	117	143	173	185
	ST평가 포함시 합계	40	-	78	106	127	169	195	225	237
	평가업무수의배율 (EAL1기준)	**0.51**	-	**1**	**1.35**	**1.63**	**2.17**	**2.5**	**2.88**	**3.04**

(*) ST평가는 모든 수준의 평가에 공통적으로 포함됨

와 같이 각 단어별 난이도를 정하였다. 결과의 객관성을 높이기 위해, 설문결과의 최대·최소값을 제외한 값의 평균을 평가난이도 가중치로 사용하였다.

표 2는 모든 보증컴포넌트에 공통적으로 나타나는 문장인 "제출물과 증거요구사항간의 만족성 확인"업무(이를 "기준업무"라 함)의 난이도를 1로 정했을 때의 다른 단어들의 상대적인 난이도이다. 예컨대, 표본검사는 기준업무에 비해 0.54배이며 모든검사는 0.78배 복잡하며 평가업무량이 많다. 또한, 취약성분석은 기준업무에 비해 6.11배 평가업무량이 많다.

본 논문에서는 표 2에서 보인 난이도 가중치를 각 보증컴포넌트에 나타난 "평가자행동"에 적용하여 다음과 같은 "보증수준별 평가업무량 산정 알고리즘"을 적용하여, 보증수준별 평가업무량의 상대적 배율을 구하였다.

[보증수준별 평가업무량 산정알고리즘]

ac_i: 보증컴포넌트 i
wac_i: ac_i의 난이도가중치(<표 2> 참조)
EAC_i: 보증컴포넌트의 평가업무량
EAL_i: 보증수준 i
$WEAL_i$: 보증수준 i의 평가업무량

```
For all component ac_i in Family in Class, do
   // 각 컴포넌트별 평가업무량 산정
   EAC_i = ac_i × wac_i ;
end_do
// j = 1, 2, 3, ..., 7
For all EAC_i in EAL_j in EAL do
// 각 보증수준별 평가업무량 산정
WEAL_j = WEAL_j + EAC_i ;
end_do
```

표 3은 각 보증수준별 평가업무량과 EAL1수준(이를 "베이스라인"이라 함)을 1로 정했을 때의 각 보증수준별 평가업무량 및 배율을 보인다. 여기서, ST평가(상대적 평가업무량 값은 70.25)는 제품별 보안요구사항명세서의 평가에 해당하며 모든 수준의 평가에서 공통적으로 포함되므로, 고려하지 않아도 된다. 즉, 보증수준별 배율에는 영향을 주지 않는다. 예컨대, EAL2는 EAL1에 비해 1.39배 평가업무량이 많으며 EAL7은 2.80배 많다. 등급간의 차이가 크지 않은 이유는 ST평가업무량이 모든 수준의 평가에 공통적으로 포함되기 때문이다.

3.2 제품유형별 평가업무량

제품유형이란 정보보호제품중 유사한 보안기능을 갖는 제품군을 의미한다. CC에서는 정보보호제품의 유형을 DB, 네트워킹, OS, 스마트카드, 접근통제 및 기타로 분류하고 있다. PP는 제품유형별로 존재하며, ST는 실제제품(예: Oracle 9i ST 등)별로 존재한다.

제품유형별 평가업무량을 산정하기 위해, 본 논문에서는 표 4와 같이 2003년 7월 현재 웹에 올라있는 33종의 PP와 67종의 ST를 입수 및 분석하였다.[7,8]

표 2. 평가난이도의 가중치

설문항목 \ 설문결과		설문결과(난이도 가중치)			
		최소	최대	평균	**평균2(최대 · 최소 제외)**
검사(check)	1. 표본검사	0.3	1	0.54	**0.54**
	2. 모든검사	0.5	1.5	0.78	**0.78**
확인 (confirm) - 충족여부의 확인	**3. 제출물과 증거요구사항간의 만족성 확인 (기준업무)**	**1**	**1**	**1.00**	**1.00**
	4. 적용 확인	1	4	1.50	**1.41**
	5. 순응 확인	1	2.5	1.47	**1.46**
	6. 부분결과 확인	1	3	1.38	**1.34**
	7. 선택적 검증 확인	1	3	1.44	**1.40**
	8. 분석 결과 확인	1	5	1.54	**1.41**
	9. 정확성 확인	1.3	3	1.74	**1.68**
	10. 일관성 확인	1	3	1.67	**1.63**
	11. 표준 준수성 확인	1	5	1.60	**1.47**
	12. 범위 확인	1	2	1.29	**1.33**
	13. 수행 확인	1	5	1.52	**1.38**
결정 - 독립적인 분석수행 필요	14. 구성여부, 실현여부 결정	1.9	6	2.34	**2.15**
	15. 낮은 내성 결정	1	7	2.75	**2.61**
	16. 중간 내성 결정	4	10	6.03	**5.92**
	17. 높은 내성 결정	7	15.26	9.85	**9.71**
	18. 종속 관계 결정	1.5	6	2.65	**2.53**
시험 (test)	19. 부분 시험	1.5	4	2.47	**2.35**
	20. 시험 결과의 표본 시험	1.5	4	2.60	**2.40**
	21. 시험 결과의 전체 시험	2	12.5	5.28	**5.24**
	22. 독립 시험	3.9	8	5.07	**4.97**
	23. 침투 시험	3	9	5.50	**5.45**
	24. 추가적 침투 시험	2	9	5.29	**5.26**
설치재현	25. 설치의 반복(재현)	1	2	1.51	**1.48**
	26. 기타	1	2	1.44	**1.49**
취약성 분석	27. 취약성 분석	4	10	5.87	**6.11**

표 3. 보증수준별 평가업무량의 상대적 배율

	PP 평가	보증수준(ST평가 포함)						
		EAL1 (베이스라인)	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
상대적 평가업무량 (ST평가업무량 70.25포함)	51.94	106.9	148.58	172.65	230.31	255.99	287.75	298.81
평가업무량 배율(EAL1은 1로함)	**0.48**	**1.00**	**1.39**	**1.62**	**2.15**	**2.39**	**2.69**	**2.80**

표 4. 본 연구에서 조사분석한 PP 및 ST수

제품 유형 (CC의분류)	제품유형 (소분류)	조사 PP수	조사 ST수
DB	DB	2	4
네트워킹	침입탐지	5	16
	VPN	3	1
	네트워크	4	14
OS	OS	4	8
스마트카드	스카트카드	1	1
접근통제	접근통제	5	9
	키복구	3	0
기타	침입탐지	3	2
	기타	3	12
계		**30**	**55**

우선, 보안기능 요구사항면에서 PP와 ST간의 관계에 대한 비교결과는 다음과 같다.

- 실제 TOE 개발시에 PP를 참조하지 않고 개발하는 경향을 보임(ST중 28%만 "PP준수선언"을 함)
- TOE 개발시 특정 PP를 참조하지는 않았지만, CC의 보안기능요구사항을 참조한 경우는 83.6%임. 즉, 대부분의 ST는 CC의 보안기능요구사항을 이용함

또한, 본 논문에서는 다음과 같이 보안기능 사용율, 기능점수 및 컴포넌트간 계층성 개념을 이용하여 제품유형별 평가업무량을 산정하였다.

우선, 본 논문에서는 제품유형별 기능요구사항을

표 5. 제품유형별 PP 및 기능요구사항의 예

제품군	발표된 PP수	공통기능	PP별 기능
X	1개	20개	0
Y	10개	5개	조합수 매우많음

표 6. 기능 증대요인별 가중치 분석결과

			단순	보통	복잡
요구사항			4.50	6.98	10.86
설계			6.60	10.23	17.27
구현	소프트웨어	명령어	3.00	4.00	6.00
		파일	3.00	5.30	9.70
		의존도여부	4.00	6.20	10.47
	하드웨어	구성	4.00	6.20	10.47
		의존도여부	3.50	5.43	9.16
테스트			7.00	10.85	18.32

조사하기 위하여 제품유형별 PP들의 기능요구사항을 조사하였으며, PP 내의 보안기능의 사용율 개념을 도입하였다. 이에 대한 근거는 다음 표 5의 예에서 보인다.

표 5에서, X제품군의 경우 발표된 PP수가 1개이므로, PP내의 기능수를 X제품군의 기능수로 보기가 어렵다는 문제점이 발생한다(향후, 또다른 PP가 개발 가능하므로). Y제품군의 경우, 발표된 10개의 PP의 공통 기능수가 5개이며 이것만을 Y제품군의 기능으로 보기는 어렵다. 그렇다고 전체 PP의 전체 기능수를 Y제품군의 기능수로 보기도 어렵다(이 경우, 발표된 PP가 많은 제품유형의 기능수가 과다하게 많아짐). 따라서, PP별 기능의 사용율 개념을 도입하여야 한다(예: 10개 PP중 8개가 보안기능 A를 사용했다면 A의 사용율은 80%).

따라서, 본 논문에서는 CC환경 및 PP개념 하에서 제품유형별 표준 기능수를 결정하기 위하여 기능요구사항의 사용율(즉, 가중평균) 개념을 도입하여 적용하였다.

또한, 본 논문에서는 보안기능 컴포넌트들간의 계층관계를 이용하여 컴포넌트들간의 가중치를 산정하였으나, 동일 클래스 및 패밀리 내에서의 계층관계만 성립하기 때문에 이 문제를 해결하기 위하여 보안기능 요구사항 클래스, 패밀리들 간의 가중치도 고려하였다. 따라서, 보안기능 요구사항 클래스, 패밀리들간의 가중치를 산정하기 위하여 소프트웨어공학의 기능점수 모델을 적용하였다. 이를 위하여 국내의 「소프트웨어사업대가의 기준」에서 고시된 [별표 3]의 기능점수 산출표를 응용하여 표 6과 같은 기능 증대요인별 난이도 가중치를 산정하였다.[9]

표 6은 실제 정보보호제품 개발 경험이 있는 개발자들로부터 설문을 통하여 설정된 값이며, 표 6을 토대로 다시 개발자들에게 설문조사를 실시하여 CC의 각 보안기능 클래스, 패밀리에 대한 가중치를 산정하였다. 분석 결과, 보안감사 클래스(FAU)의 경우, 요구사항(9.57) + 설계(14.92) + 명령어(4.00) + 파일(7.47) + 소프트웨어의존도(9.05) + 구성(4.73) + 하드웨어의존도(4.14) + 테스트(15.83) = 69.71의 가중치 결과값을 얻을 수 있다. 통신 클래스(FCO)의 경우는 58.49의 가중치 결과값을 보이며, 이는 FAU 클래스가 FCO 클래스보다 약 1.19배 가중치가 큰 것을 나타낸다. 즉, 컴포넌트의 계층관계 분석을 통한 동일한 가중치(1)을 갖는 컴포넌트라 할지라도 서로 다른 클래스 및 패밀리에 존재하는 컴포넌트간에는 서로 상이한 가중치를 갖도록 할 수 있다.

다음은 제품유형별 평가노력량 산정 알고리즘을 나타내며 표 7은 제품유형별 보안기능 사용율의 결과를 저장하는 자료구조이다.

제품유형별 평가업무량 산정알고리즘의 특성은 다음과 같다.

- 제품유형별 보안기능그룹을 파악하기 위해, 특정 제품유형별 PP들에서 사용한 "보안기능의 사용률"

표 7. 제품유형(TYPE)별 보안기능(fri)의 사용율(Ui,j)을 위한 자료구조(UTBL)

CC내의 기능컴포넌트 \ 제품유형(TYPE)	$type_1$ (DB)	$type_2$ (침입탐지)	$type_3$ (VPN)	...	$type_m$ (기타)
fr_1	U1,1	U1,2	U1,3		U1,m
...					
fr_i	Ui,1	Ui,2	Ui,3		Ui,m
...					
fr_n	Un,1	Un,2	Un,3		Un,m

[제품유형별 평가업무량 산정알고리즘]

FClass = {FAU, FCO, FCS, FDP, FIA, FMT, FPR, FPT, FRU, FTA, FTP}: 기능클래스집합
fs_i : 기능클래스 (∈ FClass). wfs_i : fs_i의 난이도가중치. WFS_i : fs_i의 평가업무량
ff_i : 기능 패밀리. wff_i : ff_i의 난이도 가중치. WFF_i : ff_i의 평가업무량
fc_i : 기능컴포넌트 i. wfc_i : fc_i의 난이도가중치. FFC_i : fc_i의 평가업무량
PP : 실제 PP집합
$TYPE$: 제품유형집합 = {DB, 침입차단, VPN, 네트워크, OS, 스마트카드, 접근통제, 키복구, 침입탐지, 기타}
PPT_i : 제품유형 $type_i$의 PP집합. ppt_i : PPT_i내의 실제 PP_i
FR_i : ppt_i에서 사용한 기능요구사항집합 (즉, $FR_i \subseteq$ FReq, FReq는 CC내의 기능요구사항 전체집합)
fr_i : FR_i내에서 기능요구사항 컴포넌트

```
For all fs_i in FClass, do
        Function Point 방법을 통해 wfs_i 획득;
end_do
For all ff_i in fs_j in FClass, do
        Function Point 방법을 통해 wff_i 획득;
end_do
For all fc_i in ff_j in fs_k in FClass, do
        컴포넌트간 계층관계를 통해 wfc_i 획득;  // wfc_i = 1 or 2 or 3
end_do
For PPT_i in TYPE, do     // 33종의 PP분석
        For all ppt_i in PPT_i, do
                FR_i 획득;
                FReq내에서 fr_i의 사용율 U_i,j계산;
                    // U_i,j = (fr_i를 사용한 PP수)÷(PPT_i내의 PP수)
                end_do
        // U_i,j는 type_i의 기능컴포넌트 j의 사용율 (0 ~ 1사이 값)
        // 사용율의 결과는 UTBL(<표 7>참조)에 저장
end_do
For all i, j, k, do
        WFC_i,j,k = wfc_i × wff_j × wfs_k
          // WFC_i,j,k는 기능클래스 fs_i내의 기능패밀리 ff_j내의 기능컴포넌트
          // fc_i의 평가업무량 가중치
end_do
For all type_p in TYPE, do
        EFF_p = 0                    // 평가업무량 초기화
        For all k, do
                EFF_p = EFF_p + WFC_*,*,k × U_k,p.
                                     // EFF_p는 제품유형 type_p의 평가업무량
        end_do
end_do
```

을 계산하였다. 예컨대, OS제품유형의 5개의 PP 중 4개의 PP만이 F1이라는 보안기능컴포넌트를 사용했다면 OS제품유형은 F1기능을 80%사용한다.

• 제품유형별 보안기능 클래스간 및 패밀리간의 상대적인 "평가업무량 가중치"를 정하기 위해, 소프트웨어 개발비 산정방법에서 사용하는 "기능점수(Function Point)" 방법을 각 클래스 및 패밀리에 적용하였다.[9,10] 예컨대, 보안감사클래스(FAU)의 평가업무량 가중치(즉, 기능점수)가 69.71 일때, 통신클래스(FCO)는 58.49이며, FAU내의 보안감

표 8. 제품유형별 평가업무량 배율

제품 유형	DB (베이스라인)	침입 차단	VPN	네트워크	OS	스마트 카드	접근통제	키복구	침입 탐지	기타
평가업무량 배율	**1.00**	0.92	1.88	1.50	1.71	1.68	1.65	1.24	0.93	1.25

사자동대응 패밀리(FAU_ARP)의 평가업무량 가중치가 51.58일때, FAU내의 보안감사분석패밀리(FAU_SAA)는 72.28이다.

- 한 보안기능 클래스내의 컴포넌트간에는 CC에서 제시한 "컴포넌트간의 계층성"을 이용하였다. 예컨대, 보안감사분석 패밀리(FAU_SAA)내의 4개의 컴포넌트는 계층성을 가지며 컴포넌트 1의 가중치는 1이며, 컴포넌트 2와 3의 가중치는 2이며, 컴포넌트 4의 가중치는 3이다.

"제품유형별 평가업무량 산정알고리즘"을 통해, 제품유형별로 분류한 33종의 실제 PP에서 사용한 보안기능요구사항 컴포넌트로부터, 보안기능사용율, 기능점수 및 컴포넌트간 계층성을 분석하여 표 8을 구하였다.

표 8은 DB 제품유형의 평가업무량(즉, 베이스라인)을 1로 정했을 때의 각 제품유형들의 평가업무량 배율이다.

3.3 보증수준 및 제품유형별 평가업무량

앞 절에서 구한 보증수준별 평가업무량과 제품유형별 평가업무량을 카테이션프로덕트하여 "보증수준 및 제품유형별" 평가업무량의 배율을 표 8과 같이 도출하였다. 이 결과는 평가기간 및 평가비의 산정시에 공수(Man-Day 또는 Man-Month) 개념으로 활용할 수 있다. 표 9에서 침입탐지제품의 EAL4등급의 평가업무량은 베이스라인(즉, DB제품의 EAL1)보다 2.00배 많음을 보인다.

Ⅳ. 관련연구 및 비교

CC자체 뿐 아니라 CCRA가입국에서도 CC의 평가비용과 평가기간에 관한 연구결과는 발견하기 어렵다. 그 이유는 CC는 정보보호시스템의 기능 및 보증수준에 대한 개발과 평가에 대한 요구사항 집합일 뿐이며, 실제의 정보보호시스템의 구현이나 평가는 개발자 및 평가자의 환경(능력, 평가도구, 인건비수준 등)에 따라 다르기 때문이라 판단된다.

본 논문에서는 이러한 특성을 고려하여 순전히 CC만을 바탕으로 하여 제품유형별 및 보증수준별 평가노력량 배수를 산정하였으며, 이 자료는 평가비용과 평가기간의 산정에 유용하게 사용될 것이다. 표 10은 기존의 연구결과들과 본 연구간의 차이를 보인다.

Ⅴ. 결 론

본 논문에서는 보증수준별 평가업무량을 산정하기 위해, CC 보증요구사항의 각 컴포넌트에 정의된 "평

표 9. 보증수준 및 제품유형별 평가업무량의 배율

보증수준별 / 제품유형별		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	1.27	1.49	1.98	2.20	2.47	2.58	1.66
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	2.72
OS	1.71	0.82	1.71	2.38	2.77	3.68	4.09	4.60	4.79	3.10
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	1.68
기타	1.25	0.60	1.25	1.74	2.03	2.69	2.99	3.36	3.50	2.27
평균	1.39	0.66	1.39	1.93	2.25	2.99	3.32	3.74	3.89	

표 10. 본 연구와 현행 KISA제도 및 KISA원가계산결과 비교

대상 / 비교기준	KISA고시자료[1]	영화회계법인의 KISA원가[11]	1998년의 연구[12]	본 연구
대상평가기준	한국 팀입차단 및 탐지시스템평가기준, [13] CC	KISA기준(2종),CC	CC 1.0(1996년)	CC 2.1(2003년 interpretation 고려)
접근방법	■ 보증수준만 고려	■ KISA의 실제 원가계산 ■ 보증수준만 고려	■ 모든 제출물 및 평가보고서의 길이, 세부내용 고려 ■ 제품유형과 일부 보증수준을 고려	■ 표준 원가계산 ■ 상향식 배움산정법 이용 ■ 보증수준과 제품유형을 동시에 고려
보증수준	■ 평가대상문서별 소요일수 고려 ■ ST평가, 보고서작성 포함 ■ 수준별 평가일 구함	■ 평가대상문서별 소요일수 고려 ■ ST평가, 보고서작성 포함 ■ 수준별 평가일 구함	■ 제출물의 예상길이 산정 → 평가업무난이도 가정 ■ 보증수준별 업무량배수 구함 ■ ST평가를 별도로 취급	■ KISA의 실제평가자를 통한 평가난이도 구함 ■ 보증수준별 업무량배수 구함 ■ ST평가를 공통으로 취급
제품유형	■ 고려하지 않음	■ 고려하지 않음	■ KISA기준: 사용자 인증, 접근통제, 바이러스 방지, 침입탐지, OS로 분류 ■ 5종의 PP를 조사	■ CC기준: DB, 네트워킹, OS, 스마트카드, 접근통제, 기타 ■ 33종의 PP, 67종의 ST를 조사 ■ PP와 ST간의 관계분석 ■ 보안기능 사용율, 기능점수, 컴포넌트 계층성 이용
보증수준과 제품유형동시 고려	■ 보증수준만 고려	■ 보증수준만 고려	일부 보증수준에대해 고려 (예: 바이러스방지제품의 경우 EAL3까지)	■ 모든 보증수준에 대해 고려함 ■ 카테이션프로덕트

가자행동" 및 "근거요구사항"을 고려하였으며, 평가경험이 있는 KISA의 직원 20명으로부터 설문조사하여 각 평가자행동에서 사용하는 "단어"별 난이도를 정하였다. 제품유형별 평가업무량을 산정하기 위해, 33종의 PP와 67종의 ST를 입수 및 분석하였고, 제품유형별 보안기능그룹을 파악하기 위해, 특정 제품유형별 PP들에서 사용한 "보안기능의 사용률"과 "기능점수" 방법을 각 클래스 및 패밀리에 적용하였다. 또한, 컴포넌트간에는 컴포넌트간의 "계층성"을 이용하였다.

PP와 ST간의 비교 분석결과, 실제 TOE 개발시에 PP를 참조하지 않고 개발하는 경향을 보이며 대부분의 ST는 CC의 보안기능요구사항을 이용하고 있다. 보증수준 및 제품유형별 평가업무량의 상대적 배수 기준은 보증수준별 평가업무량과 제품유형별 평가업무량을 카테이션 프로덕트하여 구하였다. 이 결과는 평가비와 평가기간산정의 공수개념으로 사용할 수 있다.

참 고 문 헌

[1] "정보보호시스템 평가/인증 가이드", 한국정보보호진흥원, 2002.12.

[2] CC, *Common Criteria for Information Technology Security Evaluation*, Version 2.1, CCIMB-99-031, August 1999, http://www.commoncriteria.org/site_index.html.

[3] CC, *Common Evaluation Methodology*, Version 1.0, CEM-99/045, August 1999, http://www.commoncriteria.org/site_index.html.

[4] Final Interpretations, http://www.commoncriteria.org/docs/PDF/CCPART1V21.PDF.

[5] CCRA(Arrangement on the Recognition of Common Criteria Certificates) http://www.commoncriteria.org.

[6] ISO/IEC PDTR 15446, "Information technology Security techniques - *Guide for the production of protection profiles and security targets*", Draft, Apr 3, 2000.

[7] Oracle, PP-008, *DBMS Protection Profile*, EAL3, Issue 2.1, May 2000 외 32종(기재생략).

[8] Oracle 8, Security Target, Release 8.0.5, April 2000외 66종(기재생략).

[9] 「소프트웨어사업대가의 기준」, 정보통신부 고시 2003-14호 (2003. 2. 10).

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

[11] 영화회계법인, 정보보호시스템 평가원가분석에

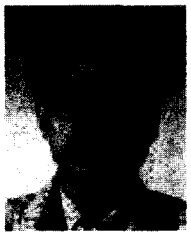
관한 위탁연구과제, KISA, 2003. 6.
[12] 이강수 외5명, EWBS를 통한 정보보호시스템의 보안성 평가업무량 및 비용산정 프로세스, 한국정보과학회논문지, 27권 2호, 2000년 2월.
[13] "정보통신망 침입차단시스템 평가기준", 정보통신부고시 제2000-14호, 한국정보보호진흥원, 2000.2.
[14] "정보통신망 침입탐지시스템 평가기준", 정보통신부고시 제2000-62호, 한국정보보호진흥원, 2000.7.

〈著者紹介〉

최 상 수 (Sang-Soo Choi) 학생회원
2001년 2월: 한남대학교 컴퓨터공학과 졸업(학사)
2003년 2월: 한남대학교 대학원 컴퓨터공학과 졸업(석사)
2003년 3월~현재: 한남대학교 대학원 컴퓨터공학과 박사과정
〈관심분야〉 소프트웨어공학, 웹공학, 보안공학, 정보보호 컨설팅 및 위험분석

최 승 (Seung Choi) 학생회원
2003년 2월: 한남대학교 컴퓨터공학과 졸업(학사)
2003년 3월~현재: 한남대학교 대학원 컴퓨터공학과 석사과정
〈관심분야〉 소프트웨어공학, 보안공학, 정보보호시스템 평가 및 보안컨설팅

이 완 석 (Wan-Suck Yi) 정회원
1991년 5월: Va. Tech 전산과학과 졸업(이학사)
1994년 8월~1996년 7월: 현대정보기술 CAD/CAM 사업부 사원
2001년 2월: 동국대학교 정보보호학과 석사
1996년 7월~현재: 한국정보보호진흥원 산업지원단 평가2팀장
〈관심분야〉 모빌코드 보안, 스마트카드 보안, 정보전, 네트워크 보안, PKI



이 강 수 (Gang-Soo Lee) 종신회원
1981년: 홍익대학교 컴퓨터공학과 졸업(학사)
1983년: 서울대학교 대학원 전산학과 졸업(이학석사)
1989년: 서울대학교 대학원 전산학과 졸업(이학박사)
1985년~1987년: 국립대전산업대학교 전자계산학과 전임강사
1992년~1993년: 미국일리노이대학교 객원교수
1995년: 한국전자통신연구원 초빙연구원
1998년~1999년: 한남대학교 멀티미디어학부장
1987년~현재: 한남대학교 컴퓨터공학과 정교수
〈관심분야〉 소프트웨어공학, 병행시스템 모형화 및 분석, 보안공학, 정보보호시스템 평가, 멀티미디어교육 커리큘럼