국내 EAL 5, 6, 7 등급의 정보보호제품 평가 인력 양성 프로세스 제안

김지선, 이윤영, 이정필, 김승주, 원동호*
성균관대학교 정보통신공학부
e-mail: jaybeam@skku.edu

A suggestion of Domestic Information Security System Evaluator training Process for EAL 5, 6, 7

Jisun Kim, Yunyoung Lee, Jungpil Lee, Seungjoo Kim, Dongho Won*
School of Information and Communication Engineering,
Sungkyunkwan University

요 약

공통평가기준(CC, Common Criteria)은 나라마다 다른 평가기준으로 인해 발생하는 시간과 비용의 문제점을 해결하기 위한 세계적인 평가 기준이다. 지난 2006년 CC 인증서 발행국이 된 우리나라는 국내 CC 평가·인증 활성화를 장려하고 있다. 하지만, CC 평가 도입 초반부터 지적된 평가 인력 수급의 문제점을 해결하지 못한 상태이다. 특별히 EAL 5, 6, 7등급의 상세한 평가 절차를 진행할 수 있는 평가 인력은 EAL 4등급 이하에 참여하는 인력과 차별되는 전문성으로 별도의 양성 대책이 필요하지만, 전반적인 인력 공급 문제에 가려 충분히 드러나지 못하였다. 본 논문은 국내 EAL 5, 6, 7등급 평가에 관련한 고등급 평가 인력의 현황을 살펴보고, 문제점을 해결하기 위한 인력 양성 프로세스를 제안한다.

1. 서론

1998년 미국을 비롯한 5개국이 참여하여 국제상호인정협정(CCRA, Common Criteria Recognition Arrangement)을 체결한 후, CC 평가·인증제도는 우리나라를 비롯한 11개국의 인증서 발행국과 13개국의 인증서 수용국에서 정보보호제품을 위한 대표적인 평가·인증 제도로 자리를 잡았다[1]. 특히 우리나라는 2008년 9월 제주도에서 열릴 CCRA세계총회 개최를 앞두고 최근 2곳의 민간 평가기관을 추가로 인가하는 등 국내 CC 평가 인증 활성화에 박차를 가하고 있다. 하지만, CC 평가 도입 초반부터 꾸준히 제기되었던 평가 인력의 부족 문제에 대해 여전히 적합한 대안을 제시하지 못한 채 평가·인증 적체 현상마저 겪고 있다[2]. 이러한 전반적인 인력 부족은 EAL 5등급 이상의 제품을 평가할 수 있는 고급 평가 인력의 부재로 이어졌다. 최근 이슈가 된 전자여권의 경우처럼 점차 디지털화되는 개인정보에 대한 보안에 높은 수준을 적용해야 한다는 목소리가 높아지면서, 일반적인 상용화 제품에서도 EAL 5등급 이상의 고등급 평가·인증을 받기 위한 시도가 꾸준히 증가할 것으로 보인다. CC 기준을 적용한 EAL 5등급 이상의 고등급 평가·인증은 특수한 목적의 보안 제품을 대상으로 하여 평가 인력의 전문성을 더욱 요구한다. 국내 최초 평가기관이자 정부 산하의 평가기관인 KISA가 최근 언론보도를 통해 "그동안 EAL 3, 4등급 평가에서 앞으로는 EAL 5, 6, 7등급 평가와 함께 스마트카드, 토큰 등 하드웨어 제품 등 고수준의 평가 위주로 진행할 계획"으로 EAL 5등급 이상의 고등급 평가 관련 기술 확보와 인력 확충에 집중할 뜻을 밝혔다[3]. 국내 EAL 5 등급 이상의 고등급 평가에 대한 투자가 필요하다는 인식에 따른 것이다.

본 논문은 국내 EAL 5, 6, 7등급 평가 인력의 현황과 문제점을 2장에서 살펴보고 3장에서 국내 EAL 5, 6, 7등급 평가 인력의 양성을 위한 구체적인 프로세스를 제시한다. 그리고 4장에서 결론을 맺는다.

2. 국내 EAL 5, 6, 7 평가 인력 현황과 문제점

2.1 EAL 5, 6, 7 등급의 평가

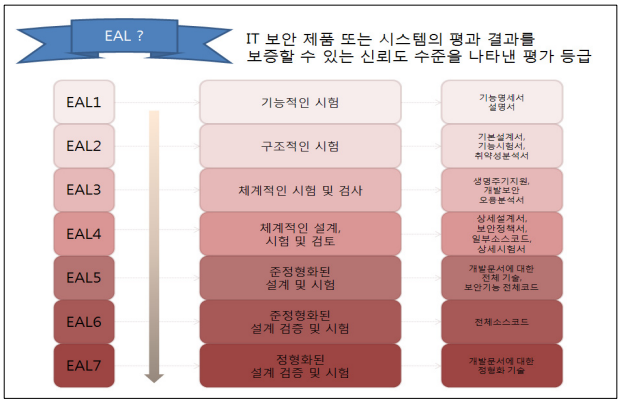
CC 평가를 통해 평가된 제품은 EAL (Evaluation Assurance Level)에 따라 등급별로 인증을 받게 된다. EAL은 IT 보안 제품 또는 시스템의 평가 결과를 책임지고 만족 시킬 수 있는 신뢰도 수준을 정의한 평가등급을 뜻한다. EAL 1부터 EAL 7까지 7등급으로 구분되며, EAL 7에 가까운 등급을 신청한 제품일수록 더 상세한 문서를 제출함과 동시에 까다로운 검증절차를 거쳐야 한다.

(그림 1)은 EAL 등급별로 수행되는 평가의 특성과 요구되는 제출물에 대한 설명을 도식화한 것이다.

EAL 5등급은 준 정형화된 설계 및 시험을 위해 개발단계에서 준 정형화된 완전한 기능명세와 모듈화 설계를 요

본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음 (IITA-2007-C1090-0701-0028)
* 교신저자 (dhwon@security.re.kr)

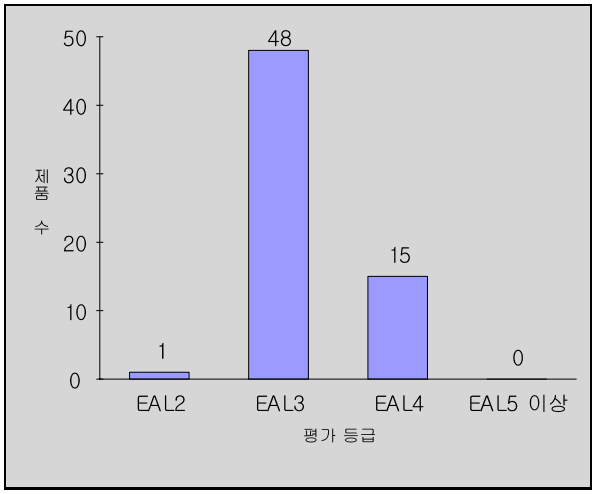
구한다. 준 정형화된 기능명세란 제한된 구문언어*와 비정형화된 설명문을 뜻한다.



(그림 1) EAL 등급별 절차와 제출물

EAL 6등급에서는 EAL 5등급의 준 정형화된 설계와 시험과 더불어 검증절차를 포함한다. 또한, 시험범위의 엄밀한 분석과 고도의 체계적인 취약성 분석, 개선된 형상관리와 정책을 요구한다. 가장 높은 등급인 EAL 7등급은 특별히 정형화된 표현, 즉 수학적인 개념에 기초한 표기와 정형화된 일치성 입증을 통한 포괄적인 시험을 추가로 요구한다. EAL 7등급 평가를 의뢰하려는 제품은 개발단계에서 정형화된 상위수준 설계 표현이 제공되는 완전한 모듈화 설계를 거쳐야 한다[4]. 국내 소프트웨어 개발환경은 EAL 5등급 이상의 고등급 평가를 위한 정형적 방법론에 아직 익숙하지 않고, 정형적 제품 설계, 검증, 분석과 개발절차에 대한 문서 역시 드물다[5]. CC 평가 도입이 얼마 되지 않은 시점에서 생소한 CC 평가 절차와 함께 이러한 정형적인 제출물을 요구하는 것은 평가 의뢰 업체에 상당한 부담이 될 것이다.

다음 (그림 2)은 CC 평가 도입 후 지난 3년간 평가 완료된 제품들의 EAL 등급을 나타낸 것이다[6].



(그림 2) 국내 CC 평가 완료 제품 등급

* 제한된 구문언어 : 제한된 문장구조와 특별한 의미의 키워드를 가진 자연어, 도식(데이터흐름도, 상태변화도, ER다이어그램, 자료구조도, 프로세스 구조도, 프로그램 구조도)

(그림 2)를 통해 국내 CC 평가 도입 이후 EAL 5등급 이상의 제품 평가는 단 한 건도 이루어 지지 않은 것을 알 수 있다. 즉, 평가기관이 EAL 5등급 이상의 고등급 평가에 대한 경험 부족으로 평가 의뢰 업체만큼이나 EAL 5등급 이상의 고등급 평가가 부담 될 것임을 짐작할 수 있다.

2.2 국내 EAL 5, 6, 7 평가 인력 현황과 문제점

CC 평가·인증 도입은 세계적인 수준의 평가 기준을 통해 국내 정보보호제품 개발환경 개선을 도모하여 경쟁력을 키우기 위함이다. 평가 의뢰 업체는 어느 정도의 부담을 피할 수 없을 것이다. 하지만, CCRA 가입 후 인증서 발행국이 된 시점에서 특정 평가 등급에 대한 평가기관의 부담은 이해하기 어렵다.

<표 1>는 국내 인증기관인 국가정보원이 정한 국내 평가 인력들의 구분을 나타낸 것이다[7].

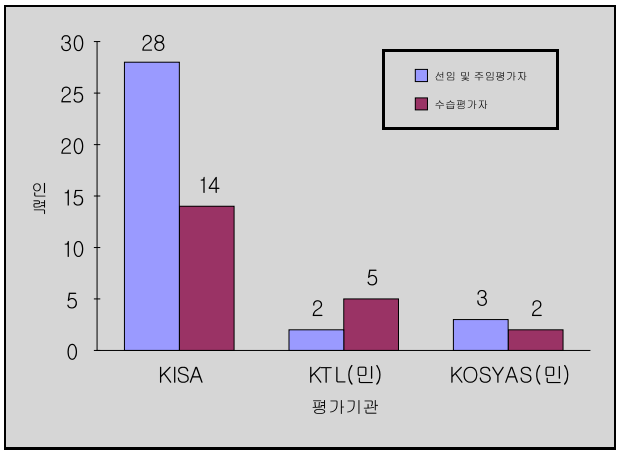
구분	자격
선임평가자	주임평가자 자격 취득 후 평가업무에 3년 이상 종사한 자로서 EAL 4 이상 등급의 평가에 2회 이상 참여한 자 또는 정보통신분야 공인시험기관에서 평가 유관업무에 5년 이상 종사한 자 중 주임평가자의 자격증을 보유한 자
주임평가자	수습평가자가 EAL3 이상의 등급 평가수행에 1회 이상 참여한 자
수습평가자	인증기관 주관으로 실시하는 평가인증관련 전문교육과정을 이수하고 시험에서 60점 이상을 득점한 자

<표 1> 국내 평가 인력 구분과 자격요건

본 논문에서 다룰 EAL 5등급 이상의 평가가 가능한 고급 평가자는 위의 구분에 따라 EAL 4등급 이상의 평가 경험이 있는 선임평가자에 가깝다. 하지만, 앞서 살펴본 대로 EAL 4등급 이하와 EAL 5등급 이상은 평가 방법과 제출물은 표현의 수준마저 다르다. 선임 평가자의 자격이 평가 수행 이력에 주로 의존하는 것은 EAL 5등급 이상의 고등급 평가의 특성을 반영하지 못한다. 게다가 이제껏 국내 EAL 5등급 이상의 제품 평가가 없었던 점을 볼 때 이러한 자격 기준은 가까운 미래 내에 EAL 5등급 이상의 고등급 평가 인력 양성을 전혀 고려하지 않은 것이다.

현재 국내 선임평가자 대부분이 CC 평가 도입 시 첫 평가기관이었던 한국정보보호진흥원의 기존 인력 중에서 차출된 경우이다. 이후 인증기관의 평가인증관련전문교육과 몇몇 대학교의 석·박사과정 교육을 통해 현재의 수습평가자와 주임평가자가 양성되었다. 인증기관이 실시한 평가인증관련전문교육과 대학의 석·박사 과정은 모두 수습평가자 양성을 목적으로 한다. 첫 번째, 평가인증관련전문교육은 일반과정과 전문과정을 구분하여 2007년 2월부터 현재까지 3개월 간격을 두고 30명씩 총 90명을 대상으로 이루어졌다. 교육기간은 10일 동안 총 80시간으로, CC 평가 전반적인 절차에 대한 내용이 주가 된다[7]. 교육과정을 모두 이수한 한 후에는 평가시험을 거쳐 합격자에 한하여 수습평가자 자격증이 교부된다. 자격증을 취득한 수습평가자 인력의 평가기관 재직은 강제 사항이 아니다. 두

번째, 몇몇 대학교의 석·박사과정에 개설된 수습평가자 양성 관련 과목* 역시 CC 평가 전반적인 절차에 대한 내용이 주가 된다. 'A'학점 이상을 수료한 학생에 한하여 수습평가자 자격을 부여한다. 다음 (그림 3)은 2007년 9월 현재 각 평가기관이 보유한 평가인력들을 나타낸 것이다.



(그림 3) 국내 평가기관별 보유 평가 인력

(그림 3)에서 볼 수 있듯이 민간평가기관을 포함한 모든 평가기관에 재직 중인 수습평가자는 총 21명이다. 평가인증관련전문교육과 대학의 석·박사 과정을 통한 수습평가자 공급 효율이 염려되는 부분이다. 실제로 대학의 석·박사과정의 경우 수료한 180명 중 실제 평가기관에서 수습평가자로 취직한 인원은 2명에 불과했다는 통계가 있다[2]. 현재 공개된 국내 CC 평가 인력 양성 방안은 평가인증관련전문교육과 대학의 석·박사 과정을 통해 양성된 수습평가자들을 주임평가자를 거쳐 선임평가자에 이르게 하는 것이다. <표 1>에서 보았던 평가자 자격요건에 따라 수습평가자가 선임평가자 되기까지 적어도 4년 이상이 걸린다. 가까운 미래 EAL 5등급 이상의 고등급 평가에 참여할 선임평가자는 현재 양성되고 있는 수습평가자들로 충원될 것이다. 하지만, 현재의 양성방안은 공급효율이 낮고 교육 내용의 전문성이 떨어져, 고등급 평가자의 자질을 보장하기 어렵다.

다음 3장에서 이러한 문제점을 해결하려는 방안을 제시하도록 한다.

3. EAL 5등급 이상의 제품 평가를 위한 고급 평가 인력 양성 프로세스

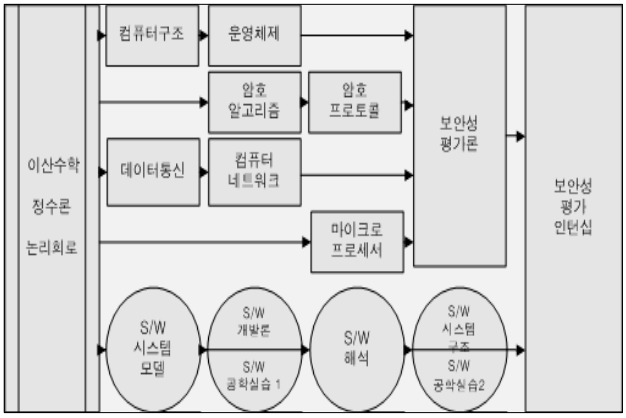
3.1 현재의 고급 평가자 양성을 위한 "CC 평가자 재교육 기관"

고급 평가 인력 양성 방안을 적용해야 할 대상을 '기존 평가자'와 '예정 평가자'로 구분하기로 한다. 첫 번째로 구분되는 '기존 평가자'란 현재 각 평가기관에 재직 중인 선임 평가자를 비롯한 EAL 3등급 이상의 평가에 참여한 주임 평가자를 포함한 것으로, CC 평가 전반에 대한 이해와 실무 경험을 보유한 인력이다. 기존 평가자를 재교육하여 고등급 평가자를 양성하는 방안은 비교적 빠른 시간에 공급할 수 있는 장점이 있다. 재교육은 외부 전문가에 위탁하여 이루어지면서 일회성보다는 주기적인 교육과정을 개설하여 이루어지는 것이 바람직하다. 다만, 복수의 평가기관 인력들을 모두 수용할 수 있어야 하므로 별도의 교육기관을 개설하여 교육하는 것을 제안한다. 별도의 교육기관은 즉, "CC 평가자 재교육 기관"으로 향후 EAL 5등급 이상의 고등급 인력을 비롯한 모든 국내 CC 평가 인력의 재교육 환경으로 활용될 수 있을 것이다. 두 번째로 구분된 '예정 평가자'는 미래의 평가 인력으로 활용될 가능성이 큰 대학의 관련 학과(예: 정보보호학, 컴퓨터 공학) 학생들을 뜻한다. CC 평가 인력의 장기적인 공급과 안정적인 발전을 위해서 대학의 관련 학과 학생을 대상으로 충분한 기간에 걸쳐 특화된 교육과정을 시행하는 것이 합리적이다. 앞서 최근 CC 평가자 양성을 위해 개설된 몇몇 대학교의 석· 박사 과정이 CC 평가 전반에 걸친 지식 전달에서 크게 벗어나지 못하여 EAL 5등급 이상의 고등급 평가자 양성과는 거리가 멀다는 것을 지적하였다. EAL 5등급 이상의 평가를 위한 고등급 평가자 양성을 위해서는 4년에 걸친 학부 과정을 통한 체계적인 교육과정이 필요하다. 이를 "CC 트랙"이라고 명시하고서 그 내용에 대해 상세히 제시하고자 한다.

3.2 미래의 고급 평가자 양성을 위한 "CC 트랙"

트랙(Track)이라는 제도는, 특정 분야가 요구하는 전문 인력 양성을 위해 설계된 교육 과정을 말한다. 이미 일부 대기업과 공공기관의 트랙 제도가 대학의 학부를 대상으로 실행되고 있다. 이러한 제도는 일반적인 대학 교육으로는 기업이나 공공기관이 원하는 전문 인력을 양성하기 어렵다는 인식을 바탕으로 한다. 의뢰 기업이나 공공기관은 대상 대학과의 협의를 거쳐, 원하는 전문 인력상을 양성하는데 필요하다고 판단되는 교과목들을 선택하거나 제시한다. 우리나라는 대학 진학률이 상당히 높고, CC 평가와 관련할 수 있는 공학 계열 대학에 대한 지원이 BK21과 같은 제도를 통해 이미 충분히 진행되어온 상태이므로, 대학 학부과정에 CC 평가 인력 양성을 위한 프로세스를 적용하는 데에 추가적인 부담이 적다. 추가적인 부담이 적다는 것은, 학부과정의 과목들에 대한 예산과 인력 지원을 추가로 하지 않아도 됨을 뜻한다. 다음 (그림 4)은 CC 트랙의 이수과정을 구성한 것이다. CC 평가자는 무엇보다 정보보호제품, 즉 보안 제품을 중점으로 평가하게 되므로 기본적인 보안기법에 대한 지식이 필요하다. 다양한 암호 알고리즘과 기법을 이해하기 하기 위한 수학적 배경지식으로 <정수론>을 먼저 이수하고 이후 한 학기 분량의 전공과목으로 <암호 알고리즘>과 <암호 프로토콜>을 이수하는 것을 권장한다[9].

* 국가정보원 IT보안인증사무국은 고려대 정보경영공학전문대학원과 성균관대 정보통신대학원과 협조해 오는 2학기부터 대학원 석·박사과정에 'IT제품 보안평가론'(3학점) 강좌를 개설, IT제품 개발 및 보안성 평가시 필요한 공통평가기준(CC) 및 평가 방법론(CEM)에 대한 이론과 실습 교육을 실시하기로 했다.



(그림 4) CC트랙 구성도

컴퓨터공학 전공과목을 포함하고 <오토마타>와 <형식언어>역시 각각 한 학기 과정으로 제시한다. <오토마타>와 <형식언어>는 EAL 5등급 제품 평가부터 요구되는 준 정형화, 정형화된 설계 검증 및 평가에 필요한 기본 과목으로 제한된 구문언어와 같은 표현 방법을 익히고 평가자로 하여금, 정형화된 제출물 해석을 위한 것이다[10]. 또한, 평가자는 S/W 제품뿐 만 아니라 H/W 제품 평가도 진행해야 하므로 H/W의 기본 지식과 관련된 전자전기학과의 <논리회로>와 <마이크로프로세서> 역시 이수한다. CC 평가는 IT 제품의 생산과 설계, 기능에 대한 분석이 주가 된다. 다양한 목적의 제품을 평가해야 하는 평가자는 이러한 분석의 공학적인 접근 능력을 길러야 한다. 외국은 이러한 공학적인 접근 능력의 중요성을 강조하며 대학교 학부 과정으로 이를 다루는 것이 대부분이다[11][12]. “CC 트랙”에서는 국내 CC 평가자의 공학적인 접근 능력을 키우고자 보통 컴퓨터공학전공에서 한 학기 전공과목으로 다루어지는 소프트웨어공학을 세분화하여 4년 학부과정 동안 학습하게 한다. 크게 <S/W 시스템 모델>, <S/W 개발론>, <S/W 해석>, <S/W 시스템구조> 4과목으로 구분하되, <S/W 개발론>과 <S/W 해석> 과목은 필요에 따라 더 세분화될 수 있다. <S/W 시스템 모델>을 통해 S/W 설계과정과 문서화에 필요한 표현기법과 모델링 기법을 교육하고, 이수 후에는 한정된 평가 제출물을 통해 제품의 전반적인 특성을 빠르게 파악할 수 있는 능력을 기르는 데에 목적을 둔다. <S/W 개발론>은 개발에 필요한 여러 가지 방법론과 그 효율성을 검증하고 판단하는 기법을 학습하여 평가 제출물을 검증하는 능력을 기른다. <S/W 해석>은 제품 산출물을 해석하고 평가하는 법을 기르기 위한 과목으로 제품 테스트과정에서 평가자에게 필요한 기술을 가르친다. <S/W 시스템 구조>는 복잡한 S/W 시스템 구조를 쉽게 구분하여 설명하는 방법을 교육한다. 이는 평가자가 주어진 평가 제품에 적합한 접근 방식을 택할 수 있는 능력을 향상시키고 평가 검증에 도움을 준다[12]. 트랙 마지막 과정에서는 <보안성평가론>과 <보안성평가인턴십>을 이수하는데, 기존의 수습평가자 교육과 유사하여 이 과정에서 트랙 참가자에게 수습평가자 자격을 부여할 것을 제안한다. “CC 트랙”은 충분한 이론적 교육과 더불어 현장교육을 병행하여, EAL 5등급 이상의 고등급 평가에 필요한 자질을 함양케 한다. 4년에 걸친 “CC 트랙”에 참여한 학생은 트랙 이수 후 실제 평가자로 활동할 확률이 높아, 효율적인 평가 인력 공급에도 역시 큰 도움이 될 것이다.

4. 결론

우리나라는 CC 평가 제도를 적용한 CCRA 가입국 중에서도 인증서를 발행할 수 있는 인증서 발행국이다. 우리나라 정보보호제품 산업의 전반적인 수준 향상을 위해서 충분히 교육받고 체계적으로 양성된 고등급 평가 인력이 필요하다. EAL 5등급 이상 제품 평가가 가능한 고등급 평가 인력은 “CC 평가자 재교육 기관”의 개설과 미래의 평가자가 될 수 있는 학부 학생들을 “CC 트랙”과 같이 특성화된 교육과정을 통해 양성하는 방법으로 양성될 수 있을 것이다. 관련 기관의 충분한 이해와 지원이 함께 한다면 이러한 제안을 활용하여 훌륭한 CC 평가 인력을 양성할 수 있으리라 본다. CCRA 가입 후, 우리나라는 국내 CC 평가・인증제도의 활성화와 국제적인 위상을 위해 많은 노력을 기울여왔다. 국내 EAL 5, 6, 7등급 평가 인력의 체계적인 양성은 국내 CC 평가・인증 인력들의 전반적인 수준을 향상시켜 이러한 노력에 빛을 더할 것이다.

참고문헌

[1] www.commoncriteriaportal.org
[2] “CC인증 평가기관, 인력-수수료문제 난항”, 보안뉴스, 2007년 9월 10일(http://www.boannews.com/)
[3] “까다로운 CC인증, 더 수월해진다.”, 보안뉴스, 2007년 7월 13일(http://www.boannews.com/)
[4] 공통평가기준 (CC 3.1) 3부. 보증요구사항
[5] “보안모델 및 메커니즘 정형검증도구 개발”, 한국정보보호진흥원, 고려대학교,
[6] 한국정보보호진흥원 보안성평가 제품 통계 (http://www.kisa.or.kr/index.jsp)
[7] 국가정보기술원 IT보안인증사무국 (http://www.kecs.go.kr/index.jsp)
[8] “민간 평가기관 1호 KTL, 인력 부족 심각”, 아이뉴스, (http://www.inews24.com/)
[9] WISE 2007 정보보호교육워크숍발표집 중 “학부과정에서 암호기술 교육: 한국기술교육대학교 사례”. 김상진.
[10] “Application and benefits of formal methods in software development” Plat, N.; van Katwijk, J.; Toetenel, H
[11] Master of Software Engineering curriculum. CMU (http://www.mse.cs.cmu.edu)
[12] “A software engineering curriculum model” Hilburn, T.B.; Bagert, D.J