6

공통평가기준에서의 EAL5 평가기준 분석

성신여자대학교 ▌서 동 수*

1. 서 론

1998년 2월부터 시행된 정보보호제품의 평가인증제도는 올해로 10년을 맞이하고 있다. 민간부문 평가를 담당하는 한국정보보호진흥원에서는 국내에서 수립된 K 등급 인증 기준에 의거하여 평가 업무를 수행하였으나 이후 국제 수준의 요구를 만족하기 위해 2002년부터 국제공통평가기준(CC: Common Criteria)[1]을 도입하여 시행해오고 있다.

2007년 4월 현재 국내에서 인증된 정보보호제품은 CC 인증과 K 등급 인증을 포함하여 모두 130여개에 이른다. 그 중 CC인증 제도에 의해 인증된 제품은 66건이며 분야별로는 네트워크 관련제품 48건, 컴퓨터 정보보호제품 15건, 그리고 정보보호기반제품 3건으로 구성되어 있다[2].

이러한 통계만 본다면 국내의 인증 수준은 다른 선진 국가들과 견주어도 손색이 없지만 인증된 제품의 등급을 보면 개선할 여지가 많아 보인다. 이들 66건의 국내 제품 중 많은 수가 평가보증등급 중 EAL(Evaluation Assurance Level) 3 이하의 인증을 받았고, EAL4 혹은 EAL4+를 포함하는 등급 제품 역시 전체의 10.6% 수준에 머물고 있다.

반면, 국외의 공통평가기준 상호인정협정(CCRA: Common Criteria Recognition Arrangement)국의 인증 추세를 살펴보면 EAL4 수준에서 벗어나 상위 수준인 EAL5 이상의 인증으로 이동하고 있음을 알 수 있다. 예로서 현재 공통평가기준의 포탈사이트[3]에 등록된 제품 중 50여개 제품이 EAL5 이상의 고등급 인증을 받았다. 젬플러스(Gemplus)사, 인피니언 테크놀러지(Infineon Technologies)사, 필립스 반도체(Philips Semiconductor)의 스마트카드 관련 운영체제 및 제어장치, 그리고 일부 IBM사의 PR/SM(Processor Resource/System Manager) 관련 제품들은 대부분 EAL5 등급을 인증 받았다. 또한 테닉스 데이터게이트(Tenix Datagate)사의 링크 데이터 다이오드 장치 관련 2개 제품이 최고 등급인 EAL7 인증을 받았다고 보고되었다.

아쉽게도 국내에서는 EAL5 이상의 인증을 신청했다거나 인증된 사례에 대한 보고가 없다. 하지만 국외의 사례에서 보듯이 스마트카드와 같은 일부 분야에 대해서는 고등급 인증이 일반화되어가고 있음을 볼 때 조만간 국내에서도 이 분야에 대한 수요가 나타날 것으로 보인다.

국제 수준의 인증 흐름을 따라가기 위해서라면 국내의 평가기관이나 기업도 EAL5 이상의 고등급 인증과 관련된 준비를 해야 할 것이다. 본 논문은 그러한 시각에서 EAL5 인증이 갖는 특징 및 유의점을 기존에 잘 알려진 EAL4와의 비교 설명을 통해 소개한다.

2. 공통평가기준의 특성

공통평가기준이란 정보보호제품의 객관적인 평가를 위해 제정된 기준으로 소프트웨어 및 시스템이 갖는 정보보호 기능에 대한 사용환경 등급을 정한 것으로서 1999년 6월 ISO 15408 표준으로 채택되었다. 공통평가기준의 개략적인 내용을 이해하기 위해서는 보호프로파일, 보안목표명세서, 평가대상 등 몇 가지 핵심이 되는 내용에 관해 살펴볼 필요가 있다.

2.1 공통평가기준의 평가대상

공통평가기준에서 말하는 평가(evaluation)란 보호프로파일, 보안목표명세서, 평가대상이 정의된 기준을 만족하는가를 판단하는 활동이라 할 수 있다. 평가에 있어 가장 중요한 대상 중의 하나인 평가대상(TOE: Target of Evaluation)이란 다름 아닌 IT제품이나 시스템, 그리고 이와 관련되는 각종 설명서들을 말한다. 보호프로파일이란 이러한 설명서 중의 하나로서 시스템 개발시 필요로 하는 보안기능의 표현에 있어 이용자들의 요구에 부합하도록 표현한 문서이다. 보안목표명세서(Security Target, ST)란 TOE가 제공하는 보안기능과 평가대상 범위를 설명하는 문서를 말한다.

그림 1은 위에서 언급된 보호 프로파일, 보안목표 명

* 정회원

세서, 평가대상(혹은 TOE) 요약서가 어떤 개발 활동에 의해 산출되는지를 보여준다. 이들에 대한 평가활동을 설명하면 다음과 같다.

1) 보호프로파일 평가: 보호프로파일이 완전하고, 일관성 있고 기술적으로 타당한지 판단하며 평가대상이 되는 TOE의 요구사항을 표현하는데 적합한지를 증명한다.
2) 보안목표명세서 평가: 보안목표명세서가 완전하고, 일관성 있고 또한 기술적으로 타당한지를 평가한다. 그리고 보안목표명세서가 보호프로파일을 수용할 경우 보호파일의 요구사항을 적절히 만족하는지를 증명한다.
3) TOE 평가: TOE가 보안목표명세서에 명세된 요구사항을 만족하는지를 증명한다.

TOE 평가 뿐 아니라 TOE에 대한 보안정책(TSP, TOE Security Policy)역시 중요한 판단 대상이다. 보안정책은 다수의 보안기능정책들로 구성되며 이들은 다시 다수의 보안기능들(SF, Security Functions)로 구현된다. 따라서 보안정책은 단독으로 설명될 수 있는 성질은 아니며 여러 개의 보안기능들의 집합으로 설명되어야 한다.

2.2 보안기능 요구사항 및 보증 요구사항

공통평가기준은 보안기능 요구사항과 보증 요구사항을 독립적인 범주로 구분한다. 보안기능 요구사항은 TOE 기능에서 요구되는 필요한 보안 행동을 정의한다. 예를 들어 식별, 인증, 암호화와 같은 기능들은 보안기능 요구사항으로 정의될 수 있다. 보증 요구사항은 보안기능들이 보안목적에 부합하는지를 나타내기 위해 최소한으로 요구되는 강도를 말한다. 예로서 기능강도에 대해 기본, 중간, 혹은 높음 등의 단계로 구분하여 요구하는 것을 생각해볼 수 있다.

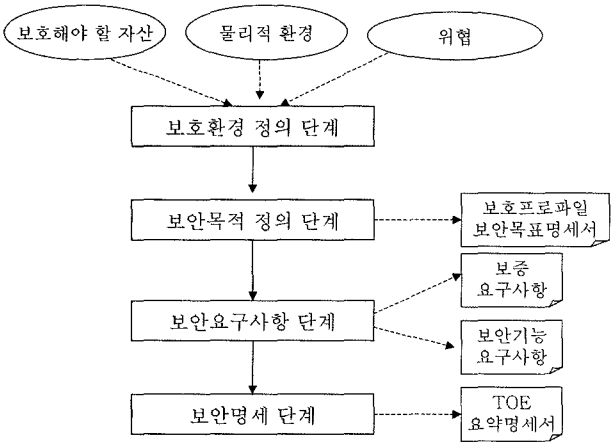

그림 1 보안 명세 단계 및 산출물

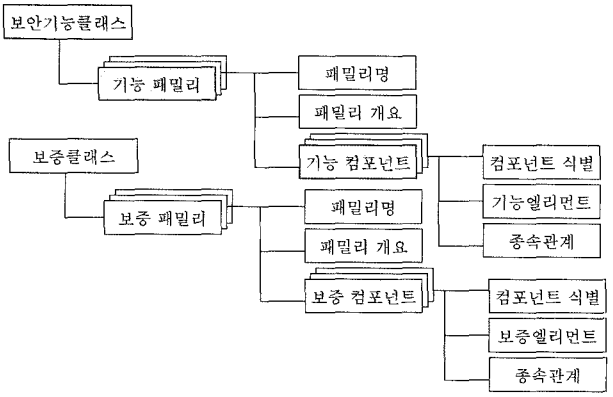

그림 2 보안 클래스의 계층구조

공통평가기준에서는 실제 보안기능 요구사항을 기능 컴포넌트라 불리는 요소에 의해 세부적으로 설명하도록 요구한다. 이 과정에서 기능 컴포넌트는 계층적인 구조에서 기능을 정의하며 명명법 또한 클래스 명, 패밀리 명, 그리고 컴포넌트 번호로 구성된 계층적 명명법을 사용한다. 보증 요구사항 역시 보안기능 요구사항의 계층 구조와 동일한 방법으로 보증 컴포넌트를 통해 표현한다(그림 2). 예를 들어 보안 감사 클래스(FAU, Security Audit) 내의 자동응답 패밀리(ARP, Automatic Response) 내의 컴포넌트 1은 FAU_ARP.1과 같은 방식으로 표기한다.

3. 보증 요구사항의 구성

보안기능 요구사항은 방화벽, VPN, 침입차단 시스템 등 각 제품 영역별로 다르게 정의되는 특성이 있다. 그러나 보증 요구사항은 개발 과정에 적용되는 개발 절차 및 문서를 판단 대상으로 하므로 제품 영역과는 독립적으로 이해될 수 있는 부분이 많다. 따라서 보편적인 적용이 가능한 보증 요구사항에 대해 설명하는 것이 개발자 혹은 평가자에게 더욱 바람직할 것으로 보인다. 본 절에서는 보증 요구사항의 구성에 관해 소개한다.

공통평가기준에서는 보증 요구사항을 7개 범주로 나누어 설명한다. 이들의 내용을 살펴보면 다음과 같다.

· 형상관리(ACM-Configuration Management): TOE 및 다른 관련 정보를 세분화하고 변경하는 과정에서 규칙적이고 체계적인 관리를 통해 TOE의 무결성이 유지됨을 보장하는데 사용된다. 이 클래스를 구성하는 보증 패밀리로는 형상관리 자동화, 형상관리능력, 형상관리 범위 패밀리가 있다.

· 배포 및 운영(ADO-Delivery and Operation): TOE의 안전한 배포, 설치, 운영에 관한 대책, 절차, 표준에 관한 요구사항을 정의한다. 이는 TOE가 전송, 설치, 시

동, 운영되는 동안 보안성이 손상되지 않음을 보장한다. 내부에는 배포 패밀리, 설치 생성 및 시도 패밀리가 있다.

· 개발(ADV-Development): 보안목표명세서의 TOE 요약명세 단계부터 실제구현 단계까지 체계적으로 세분화하기 위한 요구사항을 정의한다. 이 클래스내의 보증 패밀리로는 기능명세, 기본설계, 구현의 표현, TSF 내부, 상세설계, 표현의 일치성, 보안정책모델 등의 패밀리가 있다.

· 설명서(AGD-Guidance Document): 개발자가 제공한 운영문서의 이해용이성, 범위, 완전성에 관한 요구사항을 정의한다. 이 클래스를 구성하는 보증 패밀리는 관리자 설명서, 사용자 설명서 패밀리가 있다.

· 생명주기 지원(ALC-Lifecycle Support): 결함교정 절차 및 정책, 도구와 기법의 정확한 이용, 개발 환경을 보호하기 위한 보안 대책 등을 포함한 TOE 개발의 모든 단계에 대하여 잘 정의된 생명주기 모델을 채택함으로써 보증사항을 정의한다. 이 클래스에서 정의되는 보증 패밀리는 개발보안, 결함교정, 생명주기 정의, 도구와 기법 패밀리가 있다.

· 시험(ATE-Test): TSF가 TOE 보안기능 요구사항을 만족함을 입증하는 시험요구에 관한 사항을 설명한다. 이 클래스에서 정의되는 보증 패밀리는 범위, 상세수준, 기능시험, 독립적인 시험이 있다.

· 취약성 평가(AVA-Vulnerability Assessment): 악용가능한 취약성을 식별하는 요구사항을 정의한다. 이 클래스에서 정의되는 패밀리로는 비밀채널분석, 오용, TOE 보안기능의 강도, 취약성 분석 등의 패밀리가 있다.

그림 3은 보안기능 요구사항과 보증 요구사항 사이의 관계를 보여준다. 기능요구사항을 만족시키기 위해 확인되어야 할 대상으로는 기능명세, 기본설계, 상세설계, 그리고 구현의 표현이 있다. 각 보증 활동에 관하여는 해당되는 보증 패밀리가 정의되며 이들은 각각 ADV_FSP, ADV_HLD, ADV_LLD, ADV_IMP로 표기된다. 또한 각 활동 간의 일치성 입증을 위해서는 패밀리가, 그리고 보안정책모델이 보안기능 요구사항을 반영한 것이라는 점을 보여주기 위한 패밀리가 별도로 정의되며 이들은 각각 ADV_RCR가, ADV_SPM로 표기된다.

4. EAL4와 EAL5의 보증 클래스

본 절은 앞서 살펴본 7개의 보증 클래스를 중심으로 EAL4와 EAL5가 요구하는 클래스 요소들은 어떠한 차이를 가지는지를 설명한다.

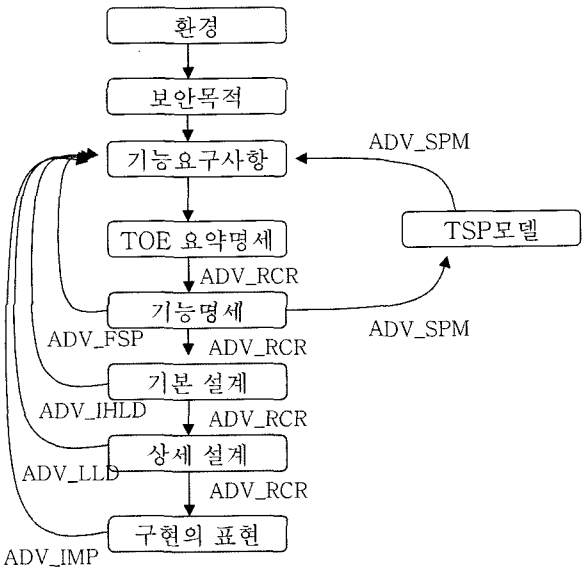

그림 3 요구사항간의 관계

공통평가기준에서 말하는 준정형화된(Semiformal) 표기란 제한된 문법과 잘 정의된 시멘틱스를 가진 언어를 사용하여 내용을 표기하는 것을 말하는 것으로 UML이나 PDL(Program Description Language), 혹은 테이블을 사용하는 표기법이 이에 속한다. EAL5는 일반적으로 준정형화된 표기법 및 개발 절차를 도입하여 활용하는 기업에서 획득할 수 있는 최고등급의 보증 수준이라고 말한다.

표 1은 보증요구사항 측면에서 EAL4와 EAL5의 요구 수준을 비교한 것으로서 앞서 언급한 7개의 클래스 별로 요구되는 항목은 어떠한 차이를 갖는지를 보여준다. 모든 클래스의 차이를 설명하는 것보다는 간결한 이해를 돕기 위해 대표적으로 개발 클래스와 생명주기지원 클래스에 국한하여 설명한다.

4.1 개발 클래스

개발 패밀리에 대해 EAL5는 TOE 보안정책의 정형화된 모델, 기능명세 및 기본설계의 준정형화된 표현, 그들 간의 준정형화된 일치성 입증을 요구한다. 또한 설계에 있어 EAL5는 모듈화된 TOE 설계를 요구한다. 여기서 주목할 점은 기능명세, 기본설계, 상세설계 등 주요 문서에서 준정형적 표기를 쓰도록 요구하지만 TOE 보안 정책에 대해서만은 정형화된 모델을 요구한다는 점이다.

정형화된 모델을 표현하기 위한 명세 언어로서 엄밀성의 정도가 높은 정형명세언어를 사용해야 한다. 정형명세 언어란 제한된 문법 뿐 아니라 수학적으로 잘 정의된 시멘틱스를 가진 표기 언어이다. 정보보호시스템의 명세로 자주 사용되는 Z나 B, HOL(Higher Order

표 1 EAL4와 EAL5의 보증 클래스 비교[2]

보증클래스	EAL4	EAL5
형상관리	ACM_AUT.1 부분적인 형상관리 자동화	EAL4와 동일
	ACM_CAP.4 생성지원 및 수용절차	EAL4와 동일
	ACM_SCP.2 문제추적 형상관리 범위	ACM_SCP.3 개발도구 형상관리범위
배포와운영	ADO_DEL.2 변경의 탐지	EAL4와 동일
	ADO_IGS.1 설치, 생성, 시동절차	EAL4와 동일
개발	ADV_FSP.2 완전히 정의된 외부 인터페이스	ADV_FSP.3 준정형화된 기본설계
	ADV_HLD.2 보안기능과 비보안 기능을 분리한 기본설계	ADV_HLD.3 준정형화된 기본설계
	ADV_IMP.1 TSF 일부에 대한 구현의 표현	ADV_IMP.2 TSF에 대한 구현의 표현
		ADV_INT.1 모듈화
	ADV_LLD.1 서술적인 상세설계	EAL4와 동일
	ADV_RCR.1 비정형화된 일치성 입증	ADV_RCR.2 준정형화된 일치성 입증
	ADV_SPM.1 비정형화된 TOE 보안정책모델	ADV_SPM.3 정형화된 TOE 보안정책모델
설명	AGD_ADM.1 관리자 설명서	EAL4와 동일
	AGD_USR.1 사용자 설명서	EAL4와 동일
생명주기 지원	ALC_DVS.1 보안대책의 식별	EAL4와 동일
	ALC_LCD.1 개발자가 정의한 생명주기모형	ALC_LCD.2 표준화된 생명주기모형
	ALC_TAT.1 잘 정의된 개발도구	ALC_TAT.2 적용된 구현표준
시험	ATE_COV.2 시험범위의 분석	EAL4와 동일
	ATE_DPT.1 기본설계 시험	ATE_DPT.2 상세설계 시험
	ATE_FUN.1 기능 시험	EAL4와 동일
	ATE_IND.2 독립시험:표본시험	EAL4와 동일
취약성평가		AVA_CCA.1 비밀채널 분석
	AVA_MSU.2 설명서 분석의 검증	EAL4와 동일
	AVA_SOF.1 TOE보안기능 강도에 관한 평가	EAL4와 동일
	AVA_VLA.2 독립적인 취약성분석	AVA_VLA.3 중간의 내성

Language)과 같은 것은 정형명세 언어의 대표적인 예라 하겠다.

기능명세(ADV_FSP)의 경우 EAL4는 ADV_FSP.2 컴포넌트를 통해 완전히 정의된 외부 인터페이스의 명세를 요구하며 또한 ADV_RCR.1 컴포넌트를 통해 이에 대한 TOE요약명세와 외부 인터페이스간의 비정형화된 일치성 입증을 요구한다. 반면 EAL5는 ADV_FSP.3 컴포넌트를 통해 준정형화된 기능명세가 적절히 되었는지를, ADV_RCR.1 컴포넌트를 통해 TOE요약명세와 준정형화된 기능명세 간에 일치성이 비정형적으로 입증 가능한지를 요구한다.

EAL4에서는 없었던 사항으로 EAL5에서는 컴포넌트 ADV_INT.1을 통해 설계정보의 모듈화를 요구한다. 이를 위해 개발자는 설계모듈간의 불필요한 상호작용을 배제한 모듈화 방식으로 보안기능을 설계했음을 보여야 한다. 모듈 내에서 개발자는 구조명세를 해야 하고 각 구조명세에는 모듈의 목적, 인터페이스, 매개변수, 효과 등이 서술되어야 한다.

EAL4는 ADV_SPM.1 컴포넌트를 통해 비정형화된 TOE 보안정책모델을 요구하는 반면 EAL5는 ADV_SPM.3 컴포넌트를 통해 정형화된 TOE모델을 요구한다. 또한 개발자는 기능명세와 정형화된 TSP 모델 간의 일치성을 입증하기위해 수학적인 증명기법을 이용해야 한다. 증명의 대상은 TSP의 모든 정책들이며 이를 적절한 수준으로 보여주기 위해서는 정형기법에서 제안한 일관성 증명, 완전성 증명 기법들을 사용해야 한다.

4.2 생명주기 정의 클래스

개발과정에서 생명주기 통제에 문제가 있다면 결함이 유입된 TOE를 사용하여 구현될 수 있다는 위험이 있다. 생명주기 정의 클래스는 이러한 위험이 제거될 수 있는 수준으로 개발과 유지를 제대로 통제하고 있는가를 판단한다.

EAL4는 ALC_LCD.1 컴포넌트를 통해 개발자가 정의한 생명주기 모델을 준수하여 개발되기를 규정한다. 반면 EAL5는 ALC_LCD.2 컴포넌트를 통해 이보다는 강화된 기준인 표준화된 생명주기모델을 준수하기를 규정한다.

표 2 각 클래스별로 요구되는 패밀리 수의 비교

보증클래스	보증패밀리	EAL3	EAL4	EAL5
형상관리	ACM_AUT		1	1
	ACM_CAP	3	4	4
	ACM_SCP	1	2	3
배포와 운영	ADO_DEL	1	2	2
	ADO_IGS	1	1	1
개발	ADV_FSP	1	2	3
	ADV_HLD	2	2	3
	ADV_IMP		1	2
	ADV_INT			1
	ADV_LLD		1	1
	ADV_RCR	1	1	2
	ADV_SPM		1	3
설명	AGD_ADM	1	1	1
	AGD_USR	1	1	1
생명주기 지원	ALC_DVS	1	1	1
	ALC_LCD	1	2	2
	ALC_TAT	1	2	3
시험	ATE_COV	2	2	2
	ATE_DPT	1	1	2
	ATE_FUN	1	1	1
	ATE_IND	2	2	2
취약성평가	AVA_CCA			1
	AVA_MSU	1	2	2
	AVA_SOF	1	1	1
	AVA_VLA	1	2	3

표 2는 보증 등급이 높아져 감에 따라 각 클래스별로 요구되는 컴포넌트의 개수에 어떠한 차이가 있는지를 비교한 것이다. 이 표에서 나타나듯이 높은 등급으로 갈수록 만족시켜야하는 보증 컴포넌트의 수가 늘어남을 알 수 있다. 음영으로 표시된 부분은 EAL4와 비교하여 EAL5가 더 많은 컴포넌트를 요구하는 부분을 표시한 것이다.

5. 결 론

본 논문은 다가올 EAL5 이상의 고등급 평가와 관련하여 EAL5 인증의 특징에 관해 소개하는 것을 목적으로 하였다. 이를 위해 공통평가기준의 중요한 두 개의 축인 보안기능 요구사항과 보증 요구사항 사이의 관계를 소개하였다. 또한 EAL4와 EAL5의 차이점을 살펴보기 위해 보증 요구사항의 중요한 구성요소인 개발과 생명주기 정의 클래스에 대한 내용을 살펴보았다.

고등급 인증은 제도와 운영 측면에서 기존의 EAL4 수준과는 차별되는 요소를 갖는다. 이것은 인증 내용을 구성하는 절차상의 차이이기도하며, 실제적인 사례를 통해 접근해야 하는 경험적인 차이이기도 하다. 예로서 스마트카드 분야는 그러한 대표적인 분야이며 영국, 프랑스, 독일 등의 국가는 고등급 시스템의 개발에 관한 경험을 쌓기 위해 이미 몇 년 전부터 유럽연합의 컨소시엄 형태로 운영되는 VerifiCard 프로젝트와 같은 대규모 프로젝트를 수행하였다. 이 과정에서 고등급 시스템의 개발은 물론 정형적 검증과 고등급 인증에 관한 다양한 기술을 축적하였다.

시기상으로 늦은 감이 없지는 않지만 우리나라에서도 EAL5 이상의 고등급 인증 기술을 확보하기 위한 거시적인 접근을 시작해야 한다고 판단한다. 이를 위해서는 중·장기적인 투자와 평가 프로젝트의 발굴, 그리고 평가 인재 육성사업이 함께 추진되어야 할 것이다.

참고문헌

[1] 정보통신부, 정보시스템 공통평가기준, 정보통신부 2002

[2] IT 보안인증사무국 http://www.kecs.go.kr

[3] Common Criteria portal http://www.commoncriteriaportal.org

[4] Gemplus, VerifiCard Final Report, 2003

서 동 수

1987 중앙대학교 컴퓨터공학과(학사)
1989 중앙대학교 컴퓨터공학과(석사)
1994 Univ. of Manchester, Dept. of Computation (석사, 박사)
1994~1998 전자통신연구원, 선임연구원
1998~현재 성신여자대학교 컴퓨터정보학부 부교수

관심분야 : 소프트웨어공학, 정형기법, 정보보호기술
E-mail : dseo@sungshin.ac.kr