프로세스 평가 모델 등급과 정보보호시스템 공통평가기준 평가보증등급 비교

김 태 훈, 이 태 승, 조규 민, 이 경 구
한국정보보호진흥원 평가기준팀

요 약

정보보호시스템 공통평가기준이 고시되고 CCRA 가입이 활발하게 추진되면서 평가보증등급(EAL)에 관한 관심이 증대되고 있다. 본 논문에서는 기존의 프로세스 평가 기준들이 취하고 있던 평가 등급과 공통평가기준의 평가보증등급을 비교함으로써 정보보호시스템 평가에 활용되고 있는 평가보증등급이 가지고 있는 특징들을 확인하였다.

The Comparison Between The Level of Process Model and The Evaluation Assurance Level

Tai-hoon Kim, Tae-seung Lee, Kyu-min Cho, Koung-goo Lee

ABSTRACT

When the Common Criteria(CC) for security system evaluation was put up, and the coming into the CCRA is promoted, the interest to the Evaluation Assurance Level(EAL) is greatly increasing. In this paper, via the comparison between the evaluation level of the exiting process evaluation criteria and the EAL of CC, the characteristics of the EAL of the CC are noted.

1. 서 론

IT 보안성 평가를 위한 정보보호시스템 공통평가기준이 2002년 8월에 고시되었으며(정보통신부 고시 제2002-40호), 향후에는 이를 이용한 정보보호시스템의 평가가 활발하게 시행될 것으로 예상되고 있다[1].

평가는 보증을 얻기 위한 전통적인 방법이며, 공통평가기준에 의한 방법론의 기초가 되는 것이다. 공통평가기준에 의한 평가의 결과는 평가보증등급(EAL, Evaluation Assurance Level)의 형태로 나타나게 되는데, 이것은 전통적인 프로세스 평가 모델인 CMM, SSE_CMM 혹은 SPICE 등에서 사용하는 등급과는 차이가 있다.

본 논문에서는 CMM, SA-CMM 등과 같은 Staged 모델 및 SSE-CMM, SPICE 등과 같은 Continuous 모델의 등급과 공통평가기준에서 정의하고 있는 평가보증등급을 비교함으로써 평가보증등급이 취하고 있는 독특한 특성을 기술하고, 이에 대한 활용 방안을 모색하여 보고자 한다.

2. 공통평가기준의 평가보증등급

공통평가기준은 신뢰를 요구하는 IT 제품 또는 시스템에 대하여 평가 결과에 기반한 보증을 제공하기 위한 것이며, 평가는 보증을 제공하는 전통적인 방법으로써 기존 평가기준에서도 기본이 되고 있다. 공통평가기준은 문서, IT 제품 또는 시스템이 갖는 정당성 및 논리성을 전문적인 평가자가 범위, 상세수준, 엄밀성의 강도를 높여가며 평가하도록 제안하고 있다. 공통평가기준의 철학은 평가에 더 많은 노력을 기울일수록 더 높은 수준의 보증이 제공되며, 최소한의 노력으로 필요한 수준의 보증을 제공해야 한다는 것이다.

평가 결과에 기반한 보증은 IT 제품 또는 시스템이 보안목적을 만족시킨다는 신뢰의 기초로 사용될 수 있고, 정확한 입증 자료가 제시되지 못하는 주장, 제품 개발과 관련된 경험 및 이용 경험 등에 의한 추상적인 보증이 아니라, 평가자의 능동적인 조사를 통한 보다 논리적인 보증을 제공하며, 이것은 다음의 <표 1>과 같은 7단계의 계층적인 평가보증등급으로 표현된다.

<표 1> 평가보증등급

보증 클래스	보증 패밀리	평가보증등급에 따른 보증 컴포넌트						
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7
형상 관리	ACM_AUT				1	1	2	2
	ACM_CAP	1	2	3	4	4	5	5
	ACM_SCP			1	2	3	3	3
배포및 운영	ADO_DEL		1	1	2	2	2	3
	ADO_IGS	1	1	1	1	1	1	1
개발	ADV_FSP	1	1	1	2	3	3	4
	ADV_HLD		1	2	2	3	4	5
	ADV_IMP				1	2	3	3
	ADV_INT					1	2	3
	ADV_LLD				1	1	2	2
	ADV_RCR	1	1	1	1	2	2	3
	ADV_SPM				1	3	3	3
설명서	AGD_ADM	1	1	1	1	1	1	1
	AGD_USR	1	1	1	1	1	1	1
생명 주기 지원	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD				1	2	2	3
	ALC_TAT				1	2	3	3
시험	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	2	2	3
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
취약성 평가	AVA_CCA					1	2	2
	AVA_MSU			1	2	2	3	3
	AVA_SOF		1	1	1	1	1	1
	AVA_VLA		1	1	2	3	4	4

3. Staged 유형 능력 성숙도 모델 등급과의 비교

3.1 Staged 유형 능력 성숙도 모델 등급의 특징

Staged 유형의 능력 성숙도 모델은 해당 등급에 속하는 핵심 프로세스 영역(KPA, Key Process Area)들을 만족하면 등급을 획득하는 형식을 취하고 있으며, 여기에 속하는 프로세스 평가 모델들은 주로 CMM 계열의 보증방법론들로서 CMM, SA-CMM, TCMM, Staged-CMMI 등이 포함된다. Staged 유형의 능력 성숙도 모델은 프로세스의 성숙 수준을 성숙도 등급(Maturity Level)으로 정의하고, 각 등급별로 수행해야 할 주요 활동을 핵심 프로세스 영역별로 목적(Goal)과 목적 달성을 위한 핵심 프로세스(Key Process)로 정의하고 있다.

3.2 Staged 유형 능력 성숙도 모델 등급과 EAL 등급의 비교

Staged 유형의 능력 성숙도 모델에서 사용하는 등급과 EAL을 비교하면 다음과 같은 유사점 및 차이점을 확인할 수 있다.

3.2.1 해당 등급에 속하는 요소들의 만족

Staged 유형 능력 성숙도 모델들이 제시하는 특정 성숙도 등급을 달성하기 위해서는 해당 등급에 속하는 핵심 프로세스 영역(KPA)들을 모두 만족하여야 하며, 이러한 내용은 기본적으로 평가보증등급이 취하는 등급 부여 방식에도 동일하게 적용된다고 할 수 있다. 즉, CMM 성숙도 등급 2에 속하는 6개의 핵심 프로세스 영역들 중에서 하나라도 만족하지 못하면 등급 2를 받지 못하는 것과 같이, 평가보증등급 2(EAL 2)에 속하는 13개의 컴포넌트 모두를 만족하지 못하면 결국 EAL 2 등급을 받지 못하게 된다.

3.2.2 하위 등급에 속하는 요소들의 만족

Staged 유형 능력 성숙도 모델의 성숙도 등급이 취하는 특성에 비추어, 획득하고자 하는 특정 성숙도 등급의 하위 등급에 속하는 모든 핵심 프로세스 영역들도 모두 만족되어야 한다는 내용도 또한 동일한 것으로 간주할 수 있다. 이것은 EAL 1에 속하는 컴포넌트들과 EAL 2에 속하는 컴포넌트들을 비교하여 봄으로써 확인할 수 있는데, 이것은 공통평가기준이 가지고 있는 컴포넌트 계층 구조의 특징에 기반한 것이며, 상위 계층의 컴포넌트는 하위 계층의 컴포넌트 내용을 모두 포함하면서 새로운 내용을 추가하는 방식이거나 하위 계층 컴포넌트의 내용을 강화하는 방식을 취하고 있기 때문에, 상위 계층의 컴포넌트를 만족한다는 것은 하위 계층의 컴포넌트를 모두 만족하는 것으로 볼 수 있는 것이다. 예를 들어, ACM_CAP.1은 1개의 개발자 관련 항목, 2개의 증거 관련 항목, 1개의 평가자 항목으로 구성되어 있다. 이에 비하여 ACM_CAP.2는 3개의 개발자 관련 항목, 6개의 증거 관련 항목, 1개의 평가자 관련 항목으로 구성되어 있으며, 이는 ACM_CAP.1에서 언급하고 있는 항목들을 모두 포함한 상태에서 추가로 다른 항목들을 포함하고 있는 형태이다. 따라서, ACM_CAP.2를 만족한다는 것은 ACM_CAP.1을 당연히 만족한다고 볼 수 있는 것이다.

3.2.3 등급 구성 요소의 차이

Staged 유형 능력 성숙도 모델에 속하는 성숙도 등급의 경우에는 각 등급에 속하는 핵심 프랙티스 영역들이 다르게 표현되어 있다. 즉, CMM 등급이 올라간다는 것은 실행하여야 하는 핵심 프로세스 영역의 수가 증가한다는 의미가 강한 것이다. 이와 달리 평가보증등급의 경

우에는 새로운 컴포넌트가 추가되는 경우도 있지만 기존 컴포넌트의 수준이 강화된다는 의미가 강하다고 할 수 있다. 예를 들어, EAL 4 등급의 경우에는 이미 대다수의 패밀리에 속하는 컴포넌트들의 수행을 요구하고 있으며, EAL 5에 이르러서는 상위 등급으로 이동하여도 더 이상 추가되는 항목이 존재하지 않고 다만 해당 컴포넌트의 보증 수준이 강화되는 형태를 나타내고 있다.

3.2.4 추가 요소가 갖는 의미의 차이

Staged 유형 능력 성숙도 모델의 경우 현재 달성한 등급의 다음 등급에 속되는 핵심 프랙티스 영역들 중의 하나 혹은 그 이상을 만족한다고 하여도 별다른 의미를 나타낸다고 표시를 하기가 어렵다. 하지만 공통평가기준의 경우에는 평가보증등급이 정의되어 있음에도 불구하고 다른 형태로 보증 컴포넌트를 조합하여 표현하는 것이 가능하다. 특히, "추가(augmentation)"라는 개념을 사용하여 특정 평가보증등급을 만족시키기 위해 달성하여야 하는 컴포넌트들 외에, 다른 보증 컴포넌트를 추가하거나 기존의 컴포넌트 수준을 강화하여 요구하는 것을 표시할 수 있다.

물론 이 경우에도 "해당 등급의 구성요소인 보증 컴포넌트를 제거한 평가보증등급"과 같은 개념은 인정되지 않으며, 보증 컴포넌트를 추가하는 경우에는 추가된 보증 컴포넌트의 유용성과 가치에 대해서도 논리적인 정당화를 인정받을 수 있어야 한다.

기존의 평가보증등급에 추가로 보증 컴포넌트를 만족하는 경우에는 등급 표시의 뒤에 '+' 기호를 사용하여 'EAL 3+' 등과 같이 표시하게 된다. 물론, 어떠한 컴포넌트가 추가되었는지는 표시할 수 없으므로 한계가 있다.

4. Continuous 유형 능력 성숙도 모델 등급과의 비교

4.1 Continuous 유형 능력 성숙도 모델 등급의 특징

Continuous 유형의 능력 성숙도 모델은 프로세스 영역(Domain)축과 수행능력(Capability)축을 나누어 고려하고 있으므로 2차원 구조 형식을 취하고 있는 것으로 볼 수 있으며, 프로세스 영역별로 수행능력 단계를 측정하여 평가한다. 여기에 속하는 프로세스 능력 성숙도 모델에는 SPICE, SE-CMM, SSE-CMM, Continuous-CMMI 등이 포함된다.

4.2 Continuous 유형 능력 성숙도 모델 등급과 EAL 등급의 비교

Continuous 유형의 능력 성숙도 모델에서 사용하는 등급과 EAL을 비교하면 다음과 같은 유사점 및 차이점을 확인할 수 있다.

4.2.1 특정 부분의 선택 가능성

2차원 구조 형식을 취하고 있는 평가 모델의 경우, 등급을 획득할 부분(프랙티스 영역)을 임의로 선택하는 것이 가능하다고 알려져 있으며, 특정 부분에서만 다른 부분에 비하여 높은 등급을 받는 것이 가능하다. 공통평가기준의 평가보증등급도 역시 특정 부분에 대하여 높은 수준을 인정받는 것이 가능한데, 이것은 '추가' 개념의 도입이 가능하기 때문이다. '추가'의 개념을 정확히 이해하고 평가받은 정보보호제품은 타 제품에 비하여 특정 부분에서 높은 보증 등급을 획득한 것으로 인정받을 수 있다. 하지만 평가보증등급의 경우에는 종속성 관계에 의하여 의도하지 않았던 컴포넌트의 추가가 발생할 수 있음에 주의하여야 한다.

4.2.2 추가 요소가 갖는 의미의 차이

물론 2차원 구조 모델의 등급과 평가보증등급이 완전히 동일한 개념으로 사용될 수는 없다. 이것은 기본적으로 평가보증등급은 특정 등급에 해당하는 모든 컴포넌트를 만족시킨다는 전제 하에, 다른 상위 등급에 속하는 컴포넌트를 추가하는 개념을 사용하기 때문이다. 다시 말해서, 추가의 개념은 특정 평가보증등급에 해당하는 컴포넌트들을 모두 만족한 상태에서 추가로 다른 컴포넌트를 만족함을 의미하는 것이다. 2차원 구조 모델의 경우에는 특정 부분만을 평가받으면서 기타 부분을 전혀 고려하지 않을 수도 있지만, 평가보증등급의 경우에는 'EAL 0'의 개념이 존재하지 않으므로 최소한 EAL 1에 해당하는 컴포넌트들은 모두 만족하여야 한다.

5. 결 론

앞서 살펴본 바와 같이 공통평가기준의 평가보증등급은 기존의 능력 성숙도 모델들이 가지고 있는 등급 구성 체계와는 다른 구조를 가지고 있다.

공통평가기준을 이용한 정보보호시스템의 보안성 평가에는 공통평가기준 3부에 있는 보증요구사항 패밀리 및 컴포넌트를 사용하여야 하는데, 이를 적절하게 활용하기 위해서는 보증 컴포넌트들로 구성된 평가보증등급의 특성을 이해할 필요가 있다.

공통평가기준의 평가보증등급은 해당 보증등급 획득 가능성 및 비용의 균형을 고려한 단계적인 척도를 제공하고 있으며, 이것은 다른 평가기준들이 채택하고 있는 등급 체계와 평가보증등급을 구분하는 중요한 이유가 된다.

공통평가기준의 평가보증등급은 Staged 모델의 특성과 Continuous 모델의 특성을 혼합한 것과 같은 독특한 특성을 가지고 있으며, 이를 기반으로 하여 특정 기관이나 기업(예를 들어 금융기관, 학교 등)에서 필요로 하는 평가보증등급을 선택하기 위한 연구가 진행될 수 있다. 또한 앞서 살펴본 평가보증등급의 특성을 고려하여 볼 때, 보호프로파일을 통하여 제시하여야 하는 보증 컴포넌트들을 선택할 경우에 정확한 이해를 바탕으로 적절한 컴포넌트를 선택하여야 할 것이다.

참고문헌

[1] 정보통신부고시 제2002-40호, 정보보호시스템 공통평가기준, 2002. 8. 5

[2] ISO/IEC 21827 Information Technology - Systems Security Engineering - Capability Maturity Model Version 2.0, 1999. 4. 1

[3] ISO/IEC JTC 1/SC 27N 3065, Guide for the Production of PPs and STs, Version 0.92, 2002. 4. 10

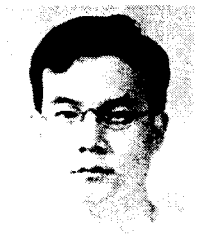
김 태 훈

1995년 성균관대학교 전기공학과(공학사)

1997년 성균관대학교 전기공학과(공학석사)

2002년 성균관대학교 전기전자및컴퓨터공학부(공학박사)

2002년 ~ 현재 한국정보보호진흥원 선임연구원



이 태 승

1994년 광운대학교 전자계산학과(공학사)

1996년 포항공과대학교 컴퓨터공학과(공학석사)

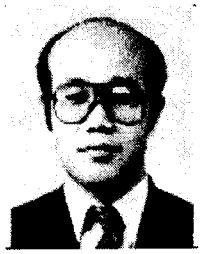
2002년 ~ 현재 한국정보보호진흥원 연구원

조 규 민

1993년 서울대학교 계산통계학과(이학사)

2002년 동국대학교 정보보호학과(공학석사)

1999년 ~ 현재 한국정보보호진흥원 선임연구원



이 경 구

1986년 University of Central Arkansas 전산학과(이학사)

1988년 University of Arkansas 전산학과(이학석사)

1996년 Kent State University 전산학과(이학박사)

1996년 ~ 현재 한국정보보호진흥원 평가기준팀장