국제공동평가기준의 평가를 받기 위한 개발자 고려사항 분석

Common Criteria Evaluations: What a Developer Should Know

김광식(K.S. Kim) 네트워크보안구조연구팀 선임연구원
남택용(T.Y. Nam) 네트워크보안구조연구팀 선임연구원, 팀장
손승원(S.W. Sohn) 네트워크보안연구부 책임연구원, 부장
박치항(C.H. Park) 정보보호연구본부 책임연구원, 본부장

본 고에서는 정보보호제품에 대한 국제공통평가기준인 CC(Common Criteria)의 적용방안에 대해 분석하였다. CC에서는 왜 보증등급에 대해 다루는지에 대한 물음에 대답하고, CC에 대해 개발자들이 알아야 할 것은 무엇인지, 그리고 기존 평가기준과의 차이점은 무엇인지에 대해 살펴보았다. CC 평가를 염두에 두고 정보보호시스템 개발을 할 경우 고려해야 할 개발자 입장에서의 이슈들에 대해 정리하고 처리방안에 대해 제시하였다. 마지막으로 제품 평가를 위한 평가과정, 평가를 위해 개발자가 준비해야 하는 개발 증거물들을 제시하고, CC에 따른 제품 평가의 효과에 대해 살펴보았다.

I. 서 론

보증 요구사항이 필요한 이유는 무엇인가? 보증은 확신의 문제이다. 보호하고자 하는 IT 제품이 놓이게 되는 보안 환경(위협, 외부 인터페이스 등)에 대해 분석한 후 이에 대한 대처를 위한 보안 기능들이 도출되고, 이에 따라 보안제품이 구현되면 된다. 만일 우리가 구현한 보안 기능이 제대로 구현되었는지에 대한 확신이 있다면 보안 제품에 대해 신뢰감을 가질 것이다. 그러나, 보안 기능이 있다고는 하는데 제대로 구현되어 있는지, 구현된 프로그램 상에 오류가 있어 취약성이 있지 않을까 하는 불안감이 들면 불필요하게 보안제품을 이중, 삼중으로 설치하고도 불안감은 없어지지 않는다. 일례로, 모 은행에서는 방화벽(firewall) 제품을 3중으로 설치하고 있다.

그러나, 만일 개발된 보안제품에 대해 만족할만한 수준의 보증이 이루어진다면 신뢰감을 가지게 된다. 보증 수준을 표현하는 것이 CC의 보증등급이다. 사용자의 요구가 너무 다양하여 보안 기능요구사항에 대해서는 기능 등급을 표현하고 있지는 않지만 [1], 보증에 대해서는 사용자의 편의를 위해 EAL (Evaluation Assurance Level)이라는 보증 패키지를 제시하고 있다. EAL 등급이 어느 정도의 보증을 하는지에 대한 수치적인 표현은 어렵지만, EAL 등급이 높아지면 그만큼 보증의 수준(확신)은 높아진다.

아래의 장에서는 CC에 대해 개발자들이 알아야 할 것은 무엇인지, 그리고 기존 평가기준과의 차이점은 무엇인지에 대해 살펴본다. CC 평가를 염두에 두고 정보보호시스템 개발을 할 경우 고려해야 할 개발자 입장에서의 이슈들에 대해 정리하고 처리방안에 대해 제시한다. 마지막으로 제품 평가를 위한 평가과정, 평가를 위해 개발자가 준비해야 하는 개

발 증거물들을 제시하고, CC에 따른 제품 평가의 효과에 대해 살펴본다.

II. CC 개념 이해

1. CC에 대해 알아야 할 것

개발자는 600페이지에 달하는 CC 규격 문서[2]를 처음부터 끝까지 읽는 것에 관심이 없으며 또한 권고되지도 않는다. CC는 주로 ST(Security Target)가 쓰여질 때 한 번 참조문서로서 사용된다[3]. ST는 CC의 모든 부분을 사용하여 쓰여져야 하며 만일 개발자가 ST를 작성한다면 CC의 모든 부분에 대해 이해하고 있어야 한다. 특히, 개발자가 사용하는 문서는 아래와 같다:

- ST 작성을 위해 Part 1 appendix C. Part 1 appendix C는 ST를 위한 필수적인 내용 요구사항을 정의하고 있다.
- 보안기능요구사항을 정의하기 위해 Part 2.
- ST를 작성하고 보안보증요구사항을 정의하기 위해 Part 3. Part 3는 EAL의 정의와 보안보증요구사항을 소개할 뿐만 아니라 ST 평가를 위한 평가 요구사항을 소개한다.

TOE(Target Of Evaluation) 평가를 위해 개발자는 CC Part 3를 이해해야만 한다. 왜냐하면 이 파트는 개발자와 평가팀의 평가요구사항을 명시적으로 명세하고 있기 때문이다. 개발자는 ST에 규정된 모든 보증요구사항을 위하여 CC Part 3에 소개된 개발자 활동 엘리먼트(세부요구사항이라고 할 수 있음)와 증거물 내용과 표현 엘리먼트에 특히 주의를 집중시켜야 한다. 이 엘리먼트들은 개발자의 의무사항에 대한 범위를 정의하고 있다. CC에서 평가자는 이 요구사항들 내에 설명되는 증거물 이상의 추가적인 증거물을 요구할 수 없다. 개발자는 보증요구사항의 평가자 활동 엘리먼트에 의한 평가자 분석의 한계에 대한 완전한 지식을 가지기 때문에, 개발자는 추가적인 증거물을 위한 비이성적인 요구에 반박할 수 있다. SFR (Security Function Requirement, 보안기능요구사항)이 CC Part 2로부터 도출되기 때문에 개발자가 CC Part 2에 대한 지식이 있어야 한다고 주장하는 사람도 있을 것이다. 만일 ST가 TOE를 위한 모든 SFR을 포함하고 있는 단독 문서라면 개발자는 CC의 요구사항들에 대비하여 ST에 있는 기능요구사항을 이해할 필요가 있다. 그러나 개발자는 가이드와 해석을 위해서만 Part 2 Annex를 참조할 필요가 있다[3].

2. 기존 평가기준과의 비교

CC는 ITSEC으로부터 직접적으로 주요 보안평가 개념의 많은 부분을 채택했는데, 가장 주목할 것은 제품 또는 시스템 평가의 기초로서 ST(보안목표명세서)를 포함하는 것이다. 그러나 ITSEC ST는 CC ST와 같지 않다. 차이점은 ITSEC ST가 CC 하에서[1] ST 평가를 받기 위해서는 CC의 증거물 내용과 표현 엘리먼트를 만족하기 위해 수정되어야 한다는 것이다. ITSEC은 보안기능 구현의 효과성과 정확성을 통해 평가 보증의 개념을 다루고 있다. CC는 CC의 Part 3에 제공되는 보안보증요구사항의 집합을 통해서 몇 가지 형식에서 모든 효과성과 정확성 보증 척도를 채택했다. <표 1>은 ITSEC, TCSEC 및 CC간의 보증 레벨의 비교를 보여 준다[4],[5]. 또한 이 비교는 ITSEC 평가 증거물의 어느 것이 CC 평가를 위해 쉽게 재사용될 수 있는지를 식별하는 데 도움을 준다.

CC에서 가장 주목할 차이는 보안기능규격 컴포넌트[2] 목록이 포함되어 있다는 것이다. 이 규격들은 IT 제품에 의해 제공되는 보안기능을 표현하기 위해 개발자에 의해 사용될 수 있는 템플릿의 집합으로 소개되고 있다. ITSEC에 비해 CC의 주요 이점은

<표 1> 보증레벨 비교

CC	EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
ITSEC	-	E1	E2	E3	E4	E5	E6
TCSEC	-	C1	C2/B1		B2	B3	A1

1) ST 평가 요구사항은 CC Part 3, 5장에 정의된다.
2) 보안 기능규격은 CC Part 2에 소개된다.

CC가 PP를 통해 구현에 독립적인 보안기능 요구사항의 집합을 제공한다는 것이다. ITSEC은 개발자나 스폰서로 하여금 보안 제품이 할 수 있는 것에 대해 자신들이 만든 보안 적용 기능의 집합을 설정하도록 하고 있다. ITSEC에서 평가된 제품들의 기능간 비교는 어려운데, 왜냐하면 하나의 제품을 위해 정의된 보안 적용 기능의 집합은 타 제품을 위한 것과 유사하지 않기 때문이다. CC를 사용함으로써 소비자는 동일 PP에 적합성이 있는 제품들의 비교를 위한 토대를 가지게 되는 장점이 있다.

III. 예상 이슈들 이해

CC 평가를 염두에 두고, 정보보호제품을 개발하고자 하는 개발자 입장에서 CC의 평가기준을 만족하기 위해 요구되는 고려사항의 일부를 열거하면 다음과 같다.

- PP/ST 작성방안
- CC 시험/평가체제 구축
- 개발환경 보안지침
- 형상관리 툴 선정, 구축 및 교육
- 개발 단계별 작성 기술 문서들 양식 및 내용 작성 방법
- 개발 단계간 일치성 검증을 위한 개발 프로세스 구축 및 적용

아래에서는 상기 6가지 이슈에 대해 고려사항을 보다 자세히 다루도록 한다.

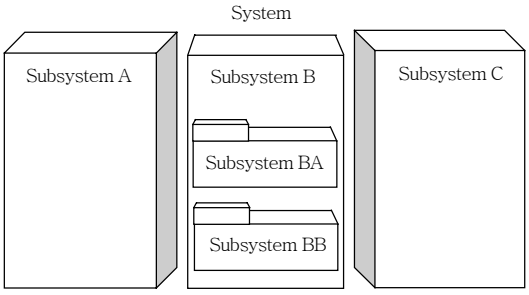
1. PP/ST 작성방안

가. PP/ST 작성을 위해 요구되는 능력

- CC의 기능 컴포넌트에 대한 이해를 하여야 한다.
- CC/EAL에 포함되는 보증 클래스(컴포넌트)에 대한 이해를 하여야 한다.
- PP/ST 작성에 도움을 주는 CC 툴박스 사용법에 대한 능력을 확보하는 것이 좋다.
- 개발하고자 하는 시스템에 대한 전반적인 지식이 있어야 한다.

나. PP/ST 작성 수준

- “개발시스템”은 하나 이상의 서브시스템으로 구성된다.
- 각 서브시스템은 TOE 대상이 될 수 있으며, 서브시스템 단위(product 수준, 예, secure engine, secure node, secure manager 등등)의 PP/ST를 작성한다.
- 새로이 PP/ST를 개발하는 것은 많은 노력이 들며, 각국의 CC 인증단체에 등록되어 있는 PP/ST를 최대한 활용한다.
- PP/ST 작성을 위해서는 (그림 1)과 같이 서브시스템 구분이 명확해야 한다.



(그림 1) 시스템과 서브시스템과의 관계

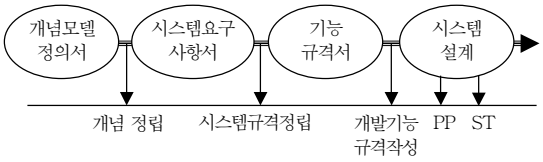
다. PP/ST 작성 전문 인력 확보 및 작업반 활용

- PP/ST 작성 업무는 기 작성되는 기능요구사항서와 기능규격서를 CC 언어로 변환하는 것이 주된 일이다.
- CC 언어에 대한 이해 능력을 높이기 위한 교육/훈련(교육기관, 자체 세미나)을 통하여 서브시스템별 PP/ST 작성을 추진한다.
- 개발에 참여하는 팀이 여럿일 경우, 각 팀별 PP/ST 작성 담당자로 구성된 작업반을 구성하여 추진한다.
- TFT 구성은 시스템 요구사항서 작성이 완료되는 시점에 본격 가동하는 것이 적절하다. 그러나,

PP 작성에 참여가 예상되는 인력은 별도의 CC 관련 교육과 지식 습득이 사전에 요구된다.

라. PP/ST 작성시점

- PP/ST 작성을 위해서는 개발하고자 하는 보안제품이 놓이게 되는 운용환경에서의 위협, 조직의 보안정책, 운용에 대한 가정사항들에 대한 분석이 먼저 이루어져야 하고, 이 분석을 통해 요구되는 보안 기능에 대한 요구사항 정의가 선행되어야 한다.
- 기능 요구사항이 개발 제품에서 만족시킬 수 있는지 여부를 확인하기 위해서는 개발 기능규격이 요구된다. 따라서, 정보보호시스템개발의 세부단계 중 기능규격의 작성이 완료되는 시점 이후에 PP를 작성하는 것이 적합하다. 그리고, 연이어서 ST를 작성하는 것이 바람직하다. 정보보호시스템 개발시 개발업체에서 채택한 순기모델에서의 PP, ST 작성 시점은 (그림 2)와 같다.



(그림 2) 순기 모델에서 PP, ST 작성시점

2. CC 시험/평가체제 구축

가. 개요

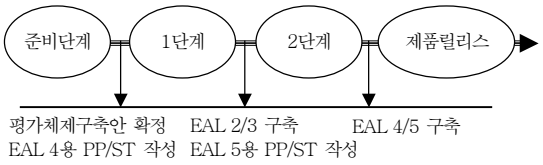
- CC에 따라 시스템을 개발하는 경우, 개발이 원하는 바대로 되었는지를 평가하기 위해서는 CEM이라는 평가방법론을 구축하여야 한다[6].
- 호환성이 요구되는 product인 경우에는 DTR (Derived Test Requirement)이라는 시험요구사항이 작성되고, 이에 따라 평가가 진행되어야 한다.

나. 평가체제 구축의 필요성

- 향후 보안 등급을 받은 정보보호제품에 대한 수요가 급증할 것을 감안한다면, 낮은 등급 수준이라도 평가할 수 있는 체제를 구축하는 것은 평가의 성공률을 높이고 평가비용을 줄이기 위해 의미가 있다고 할 수 있다.
- ISP와 같은 상업망에서는 EAL 4 또는 5등급의 높은 수준의 보안제품보다는 기존 IT 제품에 약간의 비용 추가를 통하여 어느 정도의 보증등급을 가진 보안제품에 대한 수요가 있을 것으로 생각된다.

다. 단계별 구축 방안

정보보호제품 개발에서 PP, ST, 기술문서 작성 등은 서브시스템별로 EAL 4/5 수준을 목표로 단계별로 개발하려고 한다면, (그림 3)에서 보는 바와 같이 평가체제는 정보보호제품 개발의 1단계에서는 EAL 2/3 수준으로 먼저 구축하고, 정보보호제품 개발의 2단계에 가서 EAL 4/5 수준의 평가체제를 확보하도록 한다.



(그림 3) 순기 모델에서 보증등급별 평가체제 구축시점

라. 평가체제 구축 효과

정보보호제품을 개발하면서 제품에 대한 시험 및 평가를 위한 제반사항(기술문서 작성방법, 시험 및 평가에 사용되는 평가 툴들)을 국산화하면 그만큼 정보보호제품 개발업체들의 보안제품의 시험 및 평가에 필요한 비용이 줄어들게 된다.

3. 개발환경 보안지침

가. CC 요구사항

정보보호제품이 CC/EAL 4의 요구사항을 만족하기 위해서는 순기 지원(Assurance Life Cycle:

ALC)에 대한 아래의 보증 컴포넌트의 요구사항을 만족해야 한다.

• 개발 환경에 대한 보안 척도 식별(ALC_DVS.1)

개발자는 정보보호시스템(TOE) 설계와 구현에 대한 기밀성과 무결성을 제공하기 위해 개발 환경에 대한 보안 제어 절차(개발 환경에 대한 접근 제어, 개인신상 조사, 개발 툴에 대한 보호 등)를 담고 있는 개발 보안 지침서를 제공해야 한다.

CC의 영문 규격에는 다음과 같이 되어 있다:

> Development security covers the physical, procedural, personnel, and other security measures used in the development environment. It includes physical security of the development location(s) and controls on the selection and hiring of development staff.

나. 고려사항

CC/EAL 4를 만족하는 정보보호시스템을 개발하기 위해서는 상기의 보증 컴포넌트를 만족해야 한다. 이를 위해서는

- 개발 참여자 고용시 심도 있는 신상 조사
- 개발 장소에 대한 외부인 접근제어
  - 시건장치 설치, 운용
  - 외부인 면접실 별도로 배치
- 개발 정보 유출 금지
  - 보안 지침서를 비치하여야 한다.
  - 개발자들은 보안 지침서에서 명시하는 지침을 따라야 한다.
  - 기술문서, 논문 작성 및 등록, 발표 시에 보안에 대한 심사를 받아야 한다.
- 기타 개발보안을 위해 필요한 조치사항을 검토하여 조치하여야 한다.

4. 형상관리 툴 선정, 구축 및 교육

형상(기술문서, 소프트웨어, 하드웨어)의 고유한 식별을 보장하기 위해서는 형상관리 툴을 사용하여야 한다. 세계 시장 점유율, 국내 업체 및 ETRI 내 사용상황을 보아, National사의 ClearCase 형상관리 툴을 사용하는 것이 타당할 것으로 예상한다.

5. 개발 단계별 작성 기술 문서들 양식 및 내용 작성 방법

현재, 평가방법론인 CEM에서 요구하는 세부 산출물에 대한 작성지침을 검토하고, 기술문서의 목차 정의 및 세부 목차별 작성 기준을 포함하는 정보보호 제품 개발을 위한 연구개발체계를 정립하여야 한다.

6. 개발 단계간 일치성 검증을 위한 개발 프로세스 구축 및 적용

EAL 4/5 수준의 제품개발은 보안 기능 개발의 어려움보다는 제대로 된 개발방법론의 도입과 적용이 안되기 때문에 달성이 어려운 면이 있다. 따라서, 제대로 된 개발방법론에 따라 제품을 개발하는 것이 요구된다.

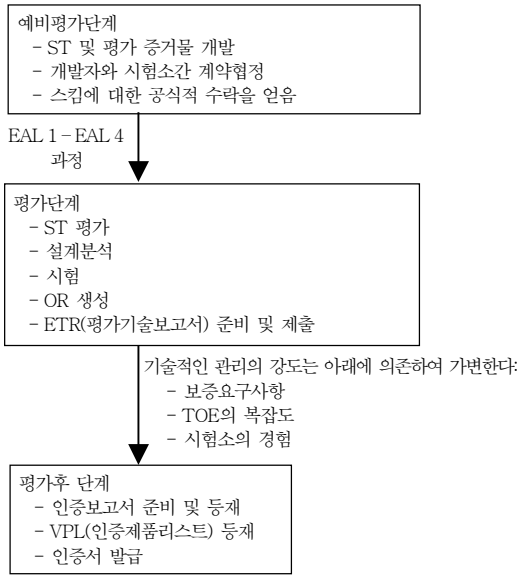
특히, 개발 세부단계간 완전한 일치성을 검증하기 위해서는 ETRI 컴소연에서 개발한 마르미 II 또는 National사의 RUP 개발방법론을 도입하는 것이 필요하다. 두 방법론 모두 UML 언어를 기반으로 하고 있는데, 두 가지 방법론 모두 지원 가능한 National사의 ROSE 제품을 도입하여 개발 프로세스에 적용하는 것을 생각할 수 있다.

IV. 제품 평가과정 이해

1. 평가과정

CC에서도 각 국가별로 독립적인 평가 스킴을 가지는 것이 가능한데, CC에서의 평가과정을 소개하기 위해 CC에 대한 선도적 역할을 하고 있는 미국의 NIAP의 평가 스킴에 따른 평가 단계를 (그림 4)에 나타내었다.

NIAP 스킴 하에서는 평가를 진행하기 앞서 인증기관에 의해 공식적으로 평가 진행에 대한 수락이 있어야 한다. 공식적인 수락을 위해서는 인증기관에



(그림 4) NIAP 스킴 평가과정

의해 ST, 평가업무계획 및 평가스케줄 검토가 요구된다. NIAP 스킴과 관련된 출판물 중 첫번째인 Common Criteria Evaluation and Validation Scheme for IT Security - Organization, Management and Concept of Operations는 각 EAL을 위한 평가 과정간의 차이를 두지는 않지만 기술적인 관리 활동의 수, 타입 및 강도를 아래에 의존해서 설명하고 있다[7]:

- ST에 있는 보증 요구사항
- TOE의 복잡도
- 식별된 기술분야에서 시험소의 IT 제품의 평가 경험

NIAP 스킴과 관련된 출판물 중 세번째인 Common Criteria Evaluation and Validation Scheme for IT Security, Technical Oversight and Validation Procedures는 기술적인 관리에 대한 특정 상세사항을 제공한다[8].

무슨 평가 과정을 따르던 간에 개발자는 그들이 평가에 들어갈 때 진행하는 수행업무의 수준을 이해해야 한다. 최소한 개발자는 아래를 위해 비용을 들이고 자원을 위임할 것이다:

- 평가되는 버전의 제품에 대해 평가자를 훈련시키고
- 평가 증거물들을 생성하고 갱신하고(아래의 평가를 위한 개발증거물 부분을 보라)
- 제품에 대한 기술적인 질문에 응답하고
- 시험소(예, 평가팀)와 인증기관과의 회의에 참석하고
- 시험 목적을 위해 제품을 제공하고
- 시험소와 계약을 관리한다.

성공적인 평가를 위하여 시험소와 개발자는 정기적으로 연락을 해야 한다. 낮은 EAL 등급 평가를 위해서 특히 더 연락이 중요한데, 왜냐하면 스케줄이 짧아서 빠른 대응과 응답은 빠듯한 스케줄을 맞추기 위해 중요하기 때문이다. 또한 비록 시험소가 제품을 평가하는 독립적인 곳이지만 개발자는 평가업무 계획에 대한 협정을 준수하기 위해 시험소와 계약제어를 가진다는 것을 명심해야 한다.

2. 평가를 위한 개발증거물

평가 증거물의 가용성과 TOE의 평가된 형상에서 TOE의 정의는 평가에서 중요하다. 개발자는 TOE로서 무엇이 평가되고 있는지 그리고 무엇이 평가된 형상인지에 대해 ST에 명확히 해야 한다. 결과적인 인증서는 평가된 형상에서 IT 제품의 특정 버전과 배포(release)에만 적용한다. <표 2>는 CC 평가를[3] 위해 요구되는 평가 증거물을 나타낸다. 이 증거물들은 평가를 위해 사용될 수 있는 상태에 있어야 한다. 증거물들은 완전하고 현재 제품을 반영하며 정확하고, 적어도 적절한 증거물의 내용과 표현 엘리먼트에 의해 명세된 대로 정보를 포함하여야 한다. 개발자는 적절하다면 다른 평가 스킴(예로써, ITSEC) 하에서 사용된 증거물을 재사용하는 것이 장려된다.

3) ○로 표시된 큰 점은 EAL을 위해 증거물이 요구된다는 의미이다. 그 다음 높은 EAL을 위해 내용에 변경이 요구되지 않으면 ○로 표시된 큰 점은 반복된다. 만일 그 다음 높은 EAL에서 내용 변경이 일어나면 + 표시가 사용된다.

<표 2> CC 평가를 위한 개발증거물

평가 증거물	EAL1	EAL2	EAL3	EAL4
Configuration Management Plan			○	+
Configuration Management Documentation	○	+	+	+
Configuration Management Acceptance Plan				○
Delivery Procedures		○	○	+
Installation, Generation, and Startup Procedures	○	○	○	○
Functional Specification	○	○	○	+
High-Level Design		○	+	○
Implementation Representation				○
Low-Level Design				○
Correspondence Analysis[4]	○	+	○	+
TOE Security Policy Model				○
Administrator Guidance[5]	○	○	+	○
User Guidance[6]	○	○	+	○
Analysis of Guidance Documentation				○
Development Security Documentation			○	○
Life-cycle Definition Documentation				○
Development Tools Documentation				○
Test Coverage Analysis		○	+	○
Test Depth Analysis			○	○
Test Documentation[7]		○	+	○
TOE Test Suite[8]		○	+	○
TOE for testing	○	○	○	○
Strength of Function Analysis		○	○	○
Vulnerability Analysis		○	○	+

4) 비록 일치성 분석을 위한 ADV_RCR.1 요구사항은 EAL 1 – EAL 4까지 동일하지만 TOE 보안기능 표현의 인접 쌍들은 EAL 2와 EAL 4에서 변경이 있다.
5) 비록 관리자 설명서를 위한 AGD_ADM.1 요구사항은 EAL 1 – EAL 4까지 동일하지만 AVA_MSU.1 요구사항은 EAL 3에서 관리자 설명서 문서를 위한 추가적인 내용 요구사항을 부과한다.
6) 비록 사용자 설명서를 위한 AGD_USR.1 요구사항은 EAL 1 – EAL 4까지 동일하지만 AVA_MSU.1 요구사항은 EAL 3에서 사용자 설명서 문서를 위한 추가적인 내용 요구사항을 부과한다.
7) 비록 시험 문서를 위한 ATE_FUN.1 요구사항은 EAL 2 – EAL 4까지 동일하지만 제공되어야 하는 정보의 양은 시험 범위분석과 시험깊이 분석에 따라서 달라진다.

필요한 모든 증거물들은 개발자가 일상적으로 이미 가지고 있는 것이 아닌 것에 주목해야 한다. 비록 EAL 1과 EAL 2 보증 요구사항은 제품개발을 위한 최상의 상업적 실행과 일치하여 증거물로서 기존의 문서를 사용하는 것이 허용되지만, CC에는 개발자가 새로운 문서 또는 추가사항을 개발하도록 하는 몇 가지 요구사항이 들어 있다. 개발자는 설치, 생성 및 시작절차, 사용자 설명서, 관리자 설명서 및 시험문서 요구사항에 주의를 기울여야 한다. 이 요구사항은 평가되는 형상에서 보안과 TOE에 관련되는 특정 설명을 요구한다. 또한, 개발자는 시험문서 요구사항을 과소평가하는 경향이 있는데, 개발자는 어떠한 평가 스케줄을 종료하기 전에 문서 요구사항을 반드시 이해하여야 한다.

마지막으로, 개발자는 평가팀이 증거물에서 문제를 찾아낸다는 것과 이 문제들을 다루는 것이 개발자의 책임이라는 것을 이해해야 한다. 개발자는 문제 해결을 위해 발생하게 되는 반복적 업무를 과소평가하지 않아야 한다. 교정 요구사항이 최종 평가 증거물에 반영됨으로써 평가팀은 요구사항을 만족한다고 증거물을 확인할 수 있다.

3. 평가의 효과

소비자가 평가된 제품을 구입함에 의해 많은 이익을 받을 것은 자명하다. 또한, 개발자는 CC의 요구사항에 대해 평가된 그들의 제품을 가짐으로 해서 수익을 올릴 것이다. 이 이익의 중요한 부분은 아래와 같다.

- CC는 국제 표준이다. 성공적인 CC 평가는 상호인정협정에 서명한 캐나다, 프랑스, 영국, 독일 및 미국과 함께 전세계적으로 인정된다. 제품은 단지 한번 평가를 받음으로써 모든 이 나라들에 의해 인정된다.

8) 비록 샘플 시험을 위한 ATE_IND.2 요구사항은 EAL 2 – EAL 4까지 동일하지만 개발자에 의해 제공되는 test suite는 시험문서에 의존한다.

- 소비자는 평가된 제품이 그것들의 보안 기능에 대해 독립적으로 제삼자 인증을 받았다는 것을 알게 된다. 개발자와 계약한 권한 있는 시험소가 평가를 수행한다.
- CC 평가는 TCSEC 평가보다 비교적 시간이 적게 수행될 것이다. 개발자는 제품의 배포사이클에 가깝게 일치하여 평가된 버전을 제공하는 것이 더 수월하게 된다.
- 성공적인 CC 평가는 정부와 민간 산업과 같은 특화된 시장에서 진입과 사용이 가능하다.
- 평가 과정은 제품의 보안 기능을 다듬고 개선하는 데 도움을 줄 것이다.
- 제품의 평가를 통해 개발자의 보안 수행이 입증되고, 개발자의 주장이 검증되게 된다.

상기와 같은 이익을 염두에 두고, 개발자는 또한 상호인정협정에 서명한 캐나다, 프랑스, 영국, 독일 및 미국에서 CC 평가가 지금 일어나고 있다는 것을 이해해야 한다. 미국의 경우, 비록 TTAP(전이프로그램) 하에서 평가가 수행되고 있지만, NIAP 스킴의 설립은 곧 된다. TTAP 하에서 발급된 인증서는 NIAP 스킴 하에서 인정될 것이다. 개발자는 CC 평가, 가용한 PP 및 평가된 제품들과 함께 최신 진행 상황을 유지하기 위해 아래의 TTAP와 NIAP 웹사이트를 방문하여야 한다: www.radium.ncsc.mil/tpep 및 www.niap.nist.gov.

V. 맺음말

본 고에서는 정보보호제품에 대한 국제공통평가기준인 CC를 정보보호제품 개발에 적용할 때 개발자들이 고려해야 할 사항들에 대해 분석하였다. CC에서는 왜 보증등급을 다루는가에 대한 물음에 대답하고, CC에 대해 개발자들이 알아야 할 것은 무엇인지, 그리고 기존 평가기준과의 차이점은 무엇인지에 대해 살펴보았다. CC 평가를 염두에 두고 정보보호 시스템 개발을 할 경우 고려해야 할 이슈들에 대해 정리하고 처리방안에 대해 제시하였다. 마지막으로 제품 평가를 위한 평가과정, 평가를 위해 개발자가 준비해야 하는 개발 증거물들을 제시하고, CC에 따른 제품 평가의 효과에 대해 살펴보았다.

정보보호 제품을 CC의 평가기준에 맞게 개발하고자 하는 개발업체의 경우, 사전에 CC의 평가등급을 만족하기 위해 무엇을 먼저 고려해야 하는지 신중히 검토할 필요가 있으며, 본 고는 검토를 위한 참고자료로 활용될 수 있을 것으로 사료된다.

참 고 문 헌

[1] 김광식, 남택용, "정보보호시스템 공통평가기준 기술동향," 전자통신동향분석, 제17권 제5호, 2002. 10., pp. 89 - 101.

[2] Common Criteria for Information Technology Security Criteria, Version 2.1, Aug. 1999.

[3] Kimberly S. Caplan and Douglas Stuart, "Common Criteria Evaluations in the US: What a Developer Should Know," Computer Sciences Corporation, 1999.

[4] Information Technology Security Evaluation Criteria, Version 1.2, June 1991.

[5] Department of Defense Trusted Computer System Evaluation Criteria, Dec. 1985.

[6] Common Evaluation Methodology for Information Technology Security, Version 1.0, Aug. 1999.

[7] Common Criteria Evaluation and Validation Scheme for Information Technology Security - Organization, Management and Concept of Operations, Scheme Publication #1, Version 2.0, dated May 1999.

[8] Common Criteria Evaluation and Validation Scheme for IT Security, Technical Oversight and Validation Procedures.