공통평가기준(CC) 시험인증제도 동향분석

임 형 수 TTA 시험인증연구소 시험인증기획팀 선임연구원
김 영 태 TTA 시험인증연구소 시험인증기획팀 책임연구원, 팀장

1. CCRA(Common Criteria Recognition Arrangment)

가. 개요

정보통신 기술과 인터넷의 발달은 정보시스템의 보급 및 활용의 급속한 증가는 물론 국경을 넘어 전 세계를 하나로 잇는 정보화 사회 구축의 기반을 조성하였다. 그러나 이러한 정보통신 기술의 발달과 급속한 정보화는 또한 정보의 유출, 위변조, 바이러스, 불건전 정보 유통, 해킹 등의 컴퓨터 범죄 등 정보화 역기능을 확산시키는 계기가 되었다. 이러한 정보화 역기능으로부터 정보시스템과 통신망을 보호하고 안전하게 운영할 수 있도록 정보보호시스템이 등장하였다.

사용자는 정보보호시스템의 평가를 통하여 안전성과 신뢰성이 검증된 정보보호시스템을 사용함으로써 조직의 정보보호 수준을 향상시켜 정보화 역기능으로부터 주요 자산의 보호에 기여하는 정보보호시스템 평가인증제도를 필요로 하게 되었다.

선진 각국에서는 정보시스템의 보안성과 신뢰도를 평가하기 위한 노력의 일환으로 자국의 실정에 맞는 정보보호시스템 평가기준을 제정하여 정부기관에서 사용되는 정보시스템을 대상으로 평가제도를 시행하였고, 민간분야에서도 안정성이 검증된 시스템의 수요가 날로 증가함에 따라 평가제도를 민간분야에까지 확장하게 되었다.

CCRA는 단일의 평가기준을 개발하여 국가간에 시행되고 있는 평가제도의 평가수준을 표준화하여 평가결과를 상호인정함으로써, 국제상호인정협정 가입국에서 평가인증받은 제품은 협정에 참여한 어떤 국가에서도 다시 평가를 거치지 않고 동일한 효력을 가질 수 있도록 하는 것이다. 이를 통해 회원국들은 일관된 제품수준 및 표준 확보, 검증된 제품의 폭넓은 선택 등 안전한 보안시스템 구축환경을 확보함과 동시에 정보보호제품 수출 시 각 국가에서 요구되는 개별 평가에 따른 시간, 비용 등의 노력을 절감할 수 있게 되었다.

CCRA는 1998년 미국, 독일, 영국, 프랑스, 캐나다 5개국이 상호국가의 보안제품 인증에 대한 협정을 기반으로 한 CCMRA(Common Criteria Mutual Recognition Arrangement)를 모체로 출발했다. 이후 2000년 미국 볼티모어에서 개최된 제1회 ICCC(International Common Criteria Conference)에서 14개 회원국을 중심으로 CCRA라는 국제보안기준 체제가 공식적으로 출범하게 되었다. 현재 24개국이 가입되어 있다. 협정에 가입했다는 것을 나타내 주는 CCRA 마크는 다음 (그림 1)과 같다.

(그림 1) CCRA 마크

나. 추진 경과

정보보호 평가기준은 정보보호시스템 신뢰도를 보증하기 위하여 정보보호시스템의 보안기능과 보증요구사항에 대한 등급기준을 정의한 기술기준으로서 미국은 1985년 제정된 TCSEC(Trusted Computer Security Evaluation Center), 유럽 4개국(영국, 프랑스, 독일, 네덜란드)은 1991년 공동으로 개발한 ITSEC(Information Technology Security Evaluation Criteria), 캐나다는 1993년 개발된 CTCPEC(Canadian Trusted Product Evaluation Criteria) 등 자국의 평가기준을 사용하여 정보보호제품을 평가하여 왔다.

하지만 평가받은 제품을 다른 평가기준을 활용하는 국가에 판매하기 위해서는 그 국가가 사용하는 평가기준을 활용하여 재평가 받아야만 수출을 할 수 있었다. 이러한 문제점을 해결하기 위해서는 국가들은 국제공통평가기준 CC 개발에 합의하였으며, 아래의 평가원칙을 항시 준수할 수 있도록 평가방법론(CEM : Common Evaluation Methodology for Information Technology Security)을 개발하여 평가자들의 평가수행에 사용할 수 있도록 하였다.

- 평가의 적절성 : 평가자들이 대상 보증평가등급(EAL : Evaluation Assurance Level)의 요구사항에 정확하게 일치하는 평가행위만을 수행하여야 한다.
- 평가의 공정성 : 모든 평가는 편견을 배제하여 수행되어야 한다.
- 평가의 객관성 : 평가결과는 주관적인 판정이나 견해가 최소화되어 얻어져야 한다.
- 평가의 반복성 및 재생산성 : 동일한 평가증거를 제시한 평가대상물 또는 보호프로파일에 대한 반복적인 평가는 항상 동일한 결과를 산출하여야 한다.
- 평가의 완전성 : 평가결과는 완전하여야 하며 기술적으로 정확하여야 한다.

이러한 원칙을 사용하여 1998년 네덜란드를 제외한 국제공통평가기준 개발에 참여한 독일, 미국, 영국, 캐나다, 프랑스 5개국은 국제공통평가기준과 평가방법론을 사용하여 평가 결과를 상호인정해 준다는 CCMRA 협정서에 서명함으로써 공식 체결되었다. 1999년 10월에는 호주와 네덜란드가 국제상호인정협정에 사인하여 총 7개 국가가 국제상호인정협정에 가입하게 되었다.

2000년 5월 미국 볼티모어에서 개최된 제1회 ICCC 컨퍼런스에서는 CCMRA 체제를 대체하는 이른바 CCRA 체제로의 변화를 거치게 되었는데, CCRA 체계가 기존의 CCMRA 체제와 크게 다른점은 단일화된 참가국 체계를 인증서 발행국과 인증서 수용국으로 이원화 했다는 데 큰 차이점이 있다. 상호인정협정 회원국 현황은 아래 〈표 1〉과 같다.

인증서 발행국인 CAP(Certificate Authorizing Participants)는 다른 국가에서 발행된 인정서를 자국에서 인정해주는 동시에 자국 내 국제상호인증협정에 의해 공인된 평가 및 인증기관을 보유하고 있는 국가로 분류되는 것을 뜻한다. 반면 인증서 수용국인 CCP(Certificate Consuming Participants)는 타국에서 발행된 인증서를 자국 내에서 인정해 주지만 자국의 평가인증제도에 의해 발행된 인증서는 타국에서 인정받지 못하는 국가를 의미한다. 현재 인증서 발행국으로는 미국, 캐나다, 영국, 독일, 프랑스, 호주, 일본, 한국 등 11개국이며 인증서 수용국으로는 이탈리아, 그리스, 핀란드, 스페인 등 12개국이 있다.

〈표 1〉 상호인정협정 회원국

구분	설명	가입국명	가입년월
인증서 발행국 (11개국)	• 인증서의 발행자인 동시에 소비국 • 평가 · 인증 체계 및 평가기관, 인증기관을 보유한 국가 • 평가인증서를 발급하는 동시에 다른 참가국이 발행한 평가인증서를 인정해 주는 국가	미국	1998. 10
		캐나다	
		영국	
		프랑스	
		독일	
		호주	1999. 10
		뉴질랜드	
		일본	2003. 10
		네덜란드	2006. 1
		노르웨이	2006. 2
		한국	2006. 5
인증서 수용국 (13개국)	• 평가인증서의 소비국 • 평가 · 인증 체계 및 평가기관, 인증기관을 보유하지 않은 국가 • 평가인증서를 발급할 수 없고, 다만 다른 참가국이 발급한 평가인증서를 수용하여 사용하는 국가	이탈리아	2000. 5
		그리스	
		핀란드	
		스페인	
		이스라엘	2000. 11
		스웨덴	2002. 2
		오스트리아	
		터키	2003. 10
		헝거리	
		체코슬로바키아	2004. 10
		싱가폴	2005. 2
		인도	2005. 4
		덴마크	2006. 6

2. CC(Common Criteria)

가. 개요

기존에 국가별로 시행하고 있던 평가인증제도에 의하면 특정 국가에서 평가인증 받은 제품은 해당 국가에서만 인정되어 타국에서 인증받기 위해서는 해당국의 평가기준에 따른 평가를 받아야 했다. 국가별 평가기준은 동일 제품의 상이한 기준에 의한 평가와 수출입시 해당국의 평가기준을 만족하는 제품이 요구될 때 중복 평가하는 문제점이 제기되었다.

이러한 문제점을 해결하고자 평가결과의 상호인정을 목표로 단일화된 공통평가기준인 CC를 제정하여 적용하게 되면 평가결과 및 시간의 절약, 평가비용의 절감에 따른 제품가격의 인하, 신속한 평가에 따른 새로운 제품개발의 가속화 등을 이룰 수 있게 된다. 이러한 점들이 CC를 개발하게 된 이유이다. CC 기준에 따라 인증된 제품에 대하여 부여되는 인증마크는 다음 (그림 2)와 같다.

(그림 2) CC 인증마크

CC 인증은 1997년에 최초로 시작되었고 2006년 11월 현재 전세계에서 CC 인증을 받은 제품은 500개 제품으로 구체적 인증제품 현황은 〈표 2〉와 같다.

〈표 2〉 CC 인증제품 현황

구분	'97	'98	'99	'00	'01	'02	'03	'04	'05	'06	계
Access Control Devices and System						1		3	7	4	15
Boundary Protection Devices and System	1	1	3	5	2	9	14	7	16	9	67
Databases		1		1	1	1	3	5	6	2	20
Data Protection			2	1	1	3	5	3	6	4	25
Detection Devices and System						1	2		4		7
ICs, Smart Card, Smart Card related Devices and System			5	11	15	20	12	23	29	17	132
Key Management System			1	1	2	3	4	5		2	18
Network and Network related Devices and System				1	1	5	2	7	13	8	37
Operating System			1	1		5	8	13	14	7	49
Products for Digital Signature								7	7	5	19
Other Devices and System					5	5	7	19	47	28	111
계	1	2	12	21	27	53	57	92	149	86	500

나. 구성

CC는 크게 세 부분으로 구성되어 있는데 제1부 소개 및 일반모델, 제2부와 제3부는 정보보호시스템에 요구되는 보안기능 요구사항 및 보안보증 요구사항으로 이루어져 있다. 보안기능 요구사항에는 보안활동을 정의하고, 보안보증요구 사항은 정보보호시스템이 보안수준에 맞게 정확하게 구현되어있는지에 대한 신뢰를 입증할 수 있는 기초를 제공하고 있다. CC의 핵심은 제2부와 제3부로 정보보호시스템이 제공해야 하는 기능 및 보증 요구사항을 기술하고 있으며 개발자는 기술된 요구사항을 참조하여 정보보호시스템을 개발할 수 있다.

구체적으로 살펴보면 제1부는 소개 및 일반모형으로써 정보보호시스템 평가원칙과 일반개념을 정의하고 평가의 일반모델을 표현하는 CC를 소개하는 부분으로, 정보보호시스템의 보안목적을 표현하고 보안요구사항을 정의하여 정보보호시스템의 상위수준 명세를 작성하기 위한 구조를 설명하고 있다.

제2부는 보안기능 요구사항으로써 평가대상의 보안기능을 표현하기 위한 기능 컴포넌트를 클래스, 패밀리, 컴포넌트의 계층관계로 구분하고 클래스의 범주를 보안감사(FAU), 통신(FCO), 암호지원(FCS), 사용자 데이터보호(FDP), 식별(인증(FIA), 보안관리(FMT), 프라이버시(FPR), TSF 보호(FPT), 자원활용(RFU), TOE 접근(FTA), 안전한 경로 · 채널(FTP)의 총 11개로 분류하였다.

제3부는 보안보증 요구사항으로써 보증평가의 척도를 정의한 평가 보증등급 EAL1~EAL7과 보증등급을 구성하는 개별적인 보증 컴포넌트, 보호 프로파일 및 보안목표 명세서 평가를 위한 기준을 포함하고 있으며, 해당 컴포넌트는 보호 프로파일 평가(APE), 보안목표 명세서 평가(ASE), 형상관리(ACM), 배포 및 운영(ADO), 개발(ADV), 설명서(AGD), 생명주기 지원(ALC), 시험(ATE), 취약성 평가

(AVA)의 클래스로 분류되어 있다.

CC는 또한 정보보호시스템 보안특성 평가에 관심을 가지는 TOE 사용자, TOE 개발자, TOE 평가자 세 집단 모두의 요구를 뒷받침할 수 있도록 구성되었다. CC의 구성과 활용은 아래 〈표 3〉과 같다

만 선택하여 쓸 수 있도록 하고 가정된 위협에 대처하기 위해 필요한 기능을 모아 놓은 정보보호제품을 보증등급(EAL)에 따라 평가한다.

이를 위해 보호 프로파일을 개발하여 인정된 보호 파일에 따라 제품을 개발하여 평가를 받거나 혹은 개발된 제품

〈표 3〉 CC의 구성과 활용

구분	사용자	개발자	평가자
1부	배경정보 및 참조목적으로 사용, 보호 프로파일 구조에 대한 지침으로 사용	TOE 보안명세를 공식화하고 요구사항을 개발하기 위한 배경정보 및 참조문헌으로 사용	배경정보 및 참조목적으로 사용. 보호 프로파일과 보안목표 명세서 구조에 대한 지침으로 사용
2부	보안기능에 대한 요구사항을 공식화하기 위한 지침이나 참조문헌으로 사용	기능요구사항을 해석하고 TOE 기능명세를 공식화하기 위한 참조문헌으로 사용	TOE가 선언된 보안기능을 만족하는지 결정하기 위한 필수적인 평가기준으로서 사용
3부	필요한 보증등급을 결정하기 위한 지침으로 사용	TOE의 보증방법을 결정하고 보증요구사항을 해석하기 위한 참조문헌으로 사용	TOE의 보안등급을 결정하고 보호 프로파일과 보안목표 명세서의 평가를 위한 필수적인 평가기준으로서 사용

다. CC 보증 등급

CC에서 정의하고 있는 등급체계는 EAL1, EAL2, EAL3, EAL4, EAL5, EAL6 및 EAL7로 구성된다. CC는 TCSEC처럼 한 등급에 대하여 기능과 보증 요구사항이 규정되어 있는 것이 아니라 다양한 기능에 필요한 요구사항을 분류하여 기준으로 제시하되 이들은 부품처럼 필요한 기능

의 개요를 보호프로파일로 구성하여 등록한 후 이에 따라 평가를 받게 된다.

CC의 보증평가등급의 경우 등급의 확장이 가능하므로 향후 기술발전에 따라 더욱 강력한 보증성을 지니는 정보보호제품이 개발될 경우에도 충분히 평가할 수 있도록 되어있으며, 국제적인 추세는 자국의 평가기준을 CC로 전환하여 수용되는 방향을 진행되고 있다. 국내외 평가기준 등급체계에 대한 비교는 아래 〈표 4〉와 같다.

〈표 4〉 국내외 평가기준 등급체계 비교

미국				캐나다	유럽		국제		한국
TCSEC		FC		CTCPEC	ITSEC		CC		침입차단 · 침입방지 시스템 평가기준
		PP	보증						
D	최소한의 보호				E0	부적절한 보증			K0
							EAL1	기능시험	K1(E)
C1	임의적 보호				E1 F-C1	비정형적 기본설계	EAL2	구조시험	K2(E)
C2	통제된 보호	CS-1	T1	T1	E2 F-C2	비정형적 상세설계	EAL3	방법론적 시험과 점검	K3(E)

미국				캐나다	유럽		국제		한국
TCSEC		FC		CTCPEC	ITSEC		CC		침입차단 · 침입방지 시스템 평가기준
		PP	보증						
B1	레이블된 보호	CS-2 CS-3 LP-1	T2 T3 T4	T2 T3	E3 F-B1	소스코드와 하드웨어 도면제공	EAL4	방법론적 설계, 시험 및 검토	K4(E)
B2	구조적 보호	LP-2	T5	T4	E4 F-B2	준정형적 기능명세서, 기본설계, 상세설계	EAL5	준정형적 설계 및 시험	K5(E)
B3	보안영역	LP-3	T6	T5	E5 F-B3	보안요소 상호관계	EAL6	준정형적 검증된 설계 및 시험	K6(E)
A1	검증된 설계	LP-4	T7	T6 T7	E6 F-B3	정형적 기능명세서, 상세설계	EAL7	정형적 검증	K7(E)

3. CC(Common Criteria) 인증절차

2006년 5월 국가정보원 IT보안인증사무국이 한국을 대표해서 CCRA에 가입함으로 인해 이전에 해외에서 받아야 했던 CC 인증을 국내에서 받을 수 있게 되었다. CC 인증에 해당하는 제품 항목은 네트워크 정보보호 기반제품, 정보보호 기반제품, 컴퓨팅 정보보호 제품 등 35개 제품이고 아래 〈표 5〉와 같다. CC 인증절차는 준비단계, 평가단계, 인증단계, 사후관리 단계로 진행되며 다음 (그림 3)과 같다.

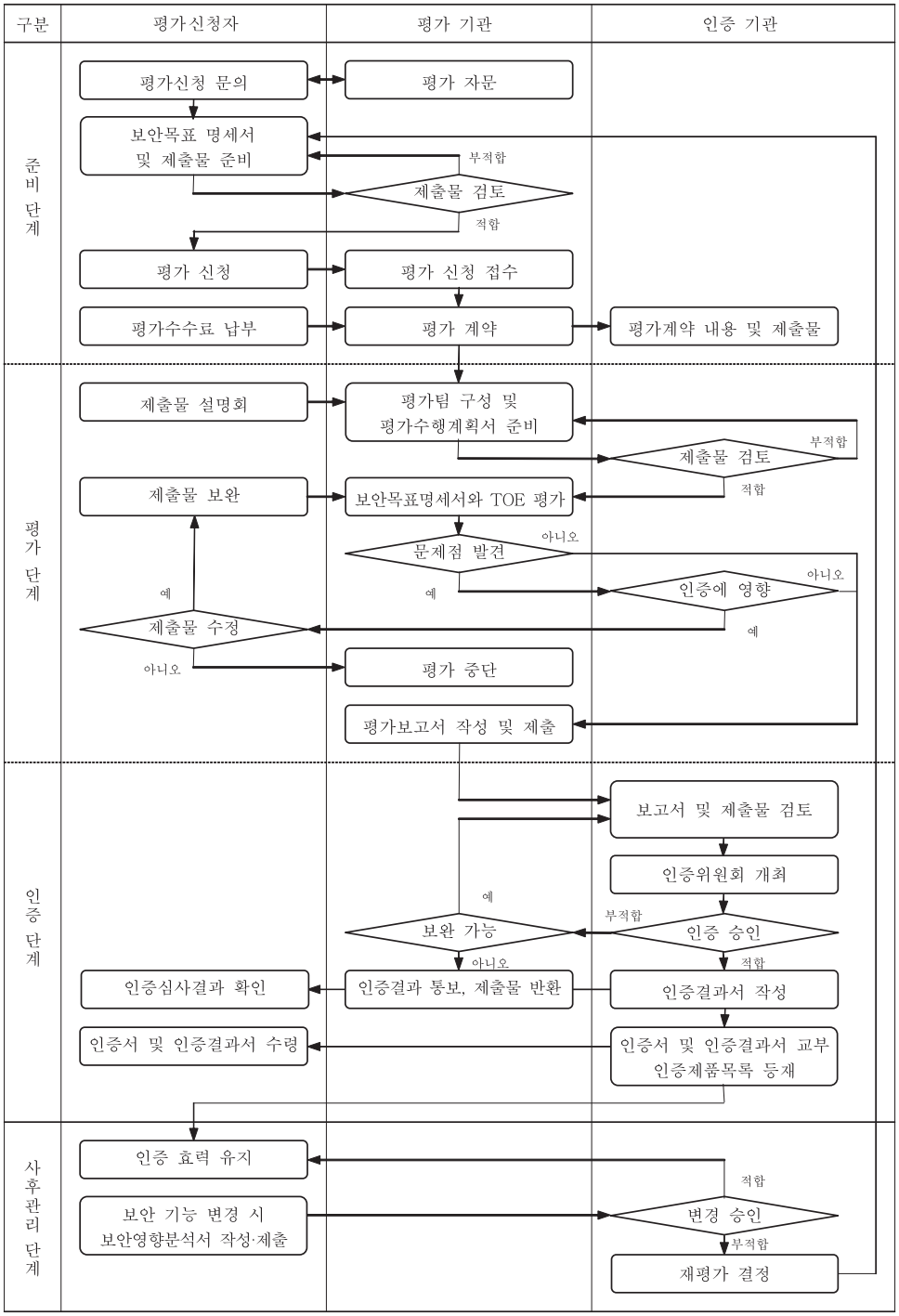
가. 준비 단계

준비 단계는 평가신청인의 평가신청부터 평가계약까지의 과정을 말한다. CC 인증을 획득하기 원하는 평가신청인은 우선 평가신청을 위한 준비 절차 등에 대해 평가 기관에 문의해 평가기관으로부터 평가신청 준비에 필요한 자문을 제공받는다.

평가신청인은 평가자문을 통해 얻은 정보를 바탕으로 평가 제출물을 완료하면 평가기관은 보호 프로파일 혹은 보

〈표 5〉 CC 인증을 받을 수 있는 제품분류

분류	장비
네트워크 정보보호제품군	라우터, 게이트웨이, 무선랜, 이동통신보안, 침입차단시스템, 망관리 시스템, 암호화 장치(전화 · 위성 · ATM), 트래픽 관리장치, 침입방지 시스템, 원격접근제어, 가상사설망, 침입탐지시스템
정보보호 기반제품	생체인식(지문, 얼굴, 홍체, 정맥), 스마트카드(칩, 운영체계, 판독기, 응용제품), 안티바이러스, 취약성 점검도구, 불건전 정보차단도구, 통신보안관리 제품, 위험분석도구, PKI
컴퓨팅 정보보호제품군	서버보안(리눅스, 유닉스, 윈도우 등), DB 보안, 메일보안, 웹서버 보안


구분
평가신청자
평가 기관
인증 기관
준비 단계
평가신청 문의
평가 자문
보안목표 명세서 및 제출물 준비
부적합
제출물 검토
적합
평가 신청
평가 신청 접수
평가수수료 납부
평가 계약
평가계약 내용 및 제출물
평가 단계
제출물 설명회
평가팀 구성 및 평가수행계획서 준비
부적합
제출물 검토
적합
제출물 보완
보안목표명세서와 TOE 평가
아니오
문제점 발견
아니오
예
인증에 영향
예
제출물 수정
아니오
평가 중단
평가보고서 작성 및 제출
인증 단계
보고서 및 제출물 검토
인증위원회 개최
예
부적합
보완 가능
인증 승인
아니오
적합
인증심사결과 확인
인증결과 통보, 제출물 반환
인증결과서 작성
인증서 및 인증결과서 수령
인증서 및 인증결과서 교부
인증제품목록 등재
사후관리 단계
인증 효력 유지
적합
보안 기능 변경 시 보안영향분석서 작성·제출
변경 승인
부적합
재평가 결정

(그림 3) CC 인증절차

안목표 명세서 등 제출물을 검토하고 평가신청인에게 평가가 제대로 이루어지고 수행될 수 있도록 보완할 부분에 대하여 조언을 한다.

평가신청인이 신청 준비가 완료되면 평가신청서를 작성하고 제출물(제품, 문서) 2부 등을 준비하여 평가신청을 한다. 평가기관은 신청인으로부터 평가신청을 접수하고 계약체결이 완료되면 인증기관에 평가 신청내용을 통보하고 평가제출물 중 1부를 인증기관에 제출한다.

나. 평가 단계

평가 단계는 평가절차의 핵심부분으로 평가계약이 체결된 후 평가팀을 구성하여 평가 제출물을 평가하고 평가보고서가 완료될 때까지의 과정이다. 평가기관은 신청된 제품을 평가하기 위해서 평가반장 및 평가자로 구성된 평가팀을 구성한다.

평가신청인은 평가 제출물에 대한 이해를 돕기 위하여 제출물 설명회를 개최하는데 제출물 설명 및 제품의 기능시연이 포함된다. 평가기관은 제출물 설명회를 통해 평가제품에 대한 평가 수행계획서를 작성하여 인증기관에 제출한다. 평가기관은 제출물 설명회를 통해 평가제품에 대해 파악한 후 평가계획서를 제출한다. 인증기관은 평가신청인과 평가기관을 참여시켜 최종 평가계획서를 협의한 후 최종 승인한다.

평가팀은 제출물을 평가하고, 평가하는 중에 평가 신청업체를 방문하여 개발환경에 대한 보안평가를 수행한다. 평가기관이 제출물 평가와 업체심사에서 발생된 문제점은 보완요청을 하면 평가 신청업체는 업체실사 및 제출물을 평가하는 동안 발생된 문제점을 보완하여 평가기관에 제출한다. 평가기관은 제출물에 대한 평가가 완료되면 평가보고서를 작성하고 인증기관에 이를 통보한다. 제출물 및 개발환경의 보완을 요청받은 신청기업이 특별한 사유없이 이에 응하지 않거나 기타 신청기업의 귀책사유로 인해 평가를 계속 진행하기가 곤란하다고 인정되는 경우 평가가 일정기간 중단되거나 평가계약이 해지된다.

다. 인증 단계

인증 단계는 인증위원회 개최를 통해 인증서 및 인증결과서를 교부하는 과정으로 진행된다. 평가기관이 평가보고서를 제출하면, 인증기관은 인증위원회를 개최하여 평가결과의 타당성 및 공정성에 대한 심의 의결 등을 수행한다.

인증위원회는 평가보고서를 검토하고 분석하여 평가수행이 CC, CEM 및 각국의 평가체계의 요구사항에 맞게 수행되었는지 확인한 후 평가결과의 적합여부를 판정하고 평가결과요약서를 작성한다. 평가결과는 평가기관과 평가신청인에게 통보한다.

인증기관은 인증위원회의 심사를 성공적으로 통과했을 경우 평가 신청인에게 인정서 및 인증결과서를 교부하고 인증된 제품에 대해 인증제품대장에 등재하여 관리한다. 평가기관은 인증된 제품의 원시 프로그램을 신청인에게 반환하며, 그외 제출물은 인증서의 유효기간 동한 안전하게 보관한다.

라. 사후 관리

신청 기업은 인증제품이 변경된 경우 보안영향 분석서를 작성하여 인증효력유지 신청을 해야 하고 인증기관은 변경내용을 검토하여 변경승인 또는 재평가 결정을 내린다. 변경이 승인된 경우 인증의 효력이 유지되고 재평가가 결정된 경우 신청기관은 평가기관에 재평가를 신청하여야 한다.

〈약어표〉

ATM – Asynchronous Transfer Mode
CAP – Certificate Authorizing Participants
CC – Common Criteria
CCP – Certificate Consuming Participants
CCEB – CC Editorial Board

CCIB – Common Criteria Implementation Board
CCIMB – Common Criteria Interpretation and Maintenance Board
CCMRA – Common Criteria Mutual Recognition Arrangement)
CCRA – Common Criteria Recognition Arrangement
CEM – Common Evaluation Methodology for Information Technology Security
CTCPEC – Canadian Trusted Product Evaluation Criteria)
EAL – Evaluation Assurance Level
ITSEC – Information Technology Security Evaluation Criteria)
PKI – Public Key Infrastructure
TCSEC – Trusted Computer Security Evaluation Center

〈참고 문헌〉

1. Common Criteria Portal site, http://www.commoncriteriaportal.org
2. 한국정보보호진흥원 website, http://www.kisa.or.kr
3. CCRA management committee, 'Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security', 2000. 5
4. 'Common Criteria', CCMB, 2005. 8
5. 'Common Methodology for Information Technology Security Evalution', CCMB, 2005. 8
6. 경영과 컴퓨터, 'CCRA 체계와 CC 인증', 제16권 14호 통권352호
7. '정보보호시스템 평가 · 인증 가이드', 한국정보보호진흥원, 2004. 12 TTA