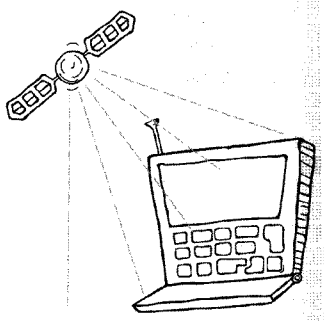
CC 평가 · 인증 동향



이은경 | TTA 시험인증연구소 SW시험인증센터 선임연구원

1. 머리말

CC(공통평가기준, Common Criteria)는 IT 제품의 보안성을 평가하기 위해 국제적으로 동의한 프레임워크로서, IT 제품이 제공하는 보안기능성(Security Functionality)과 IT 제품에 적용되는 보증수단(Security Measure)을 표준화된 방식으로 정의할 수 있는 보안요구사항을 제시한다. CC는 3부로 구성된 국제표준(ISO/IEC 15408)이며 현재 IT 제품의 신뢰성인 정보 보증(Information Assurance)을 얻기 위해 수행되는 IT 제품 보안성 평가 · 인증 제도에 가장 많이 적용되는 기준 중 하나이다.

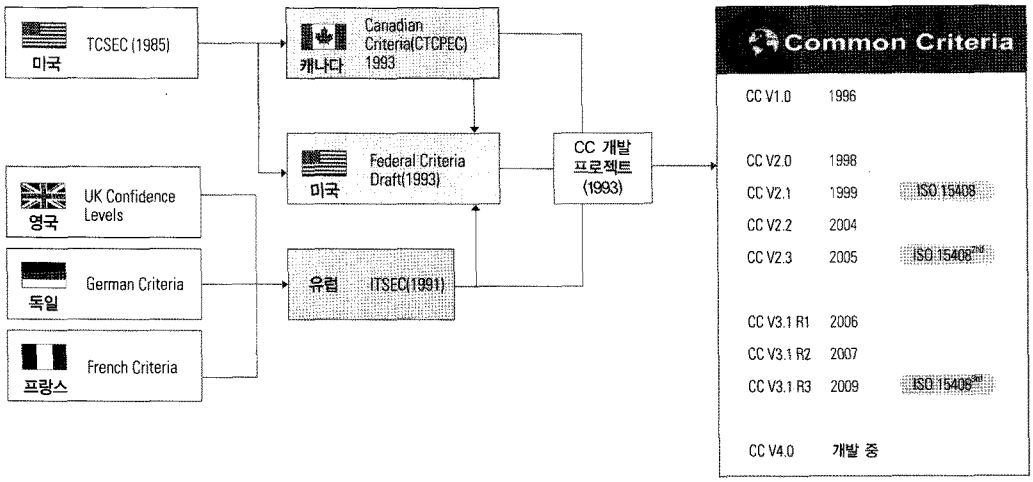
CC를 적용해 평가할 수 있는 IT 제품은 하드웨어, 펌웨어, 소프트웨어 등 다양한 형태로 구현될 수 있으며 제품으로 만들어지지 않는 특정 기술이나 IT 제품의 일부분 또는 여러 IT 제품이 결합된 형태의 평가에도 적용 가능하다.

따라서 CC는 IT 제품의 보안성을 평가하기 위한 방법으로써 유연하게 사용될 수 있으며, 보안기능성이 있는 IT 제품의 평가뿐만 아니라 IT 제품의 개발 또는 조달을 위한 지침으로 활용될 수 있다.

IT 제품이 평가기준에 부합하는지 제3자가 평가하고 공신력 있는 국가기관에 의해 평가기준 및 평가방법론이 정확하게 적용되었는지 인증함으로써 안전성 및 신뢰성이 검증된 IT 제품을 사용하도록 권고하는 평가 · 인증 제도는 과거 대부분의 국가에서 정부기관의 사용 목적을 중심으로 운영되어 왔으나 기술의 발전과 민간 분야에서 사용되는 IT 제품의 확산에 따라 정보 보증에 대한 중요성이 민간 분야까지 확대되고 있는 실정이다.

CC는 국가별로 상이한 평가기준을 적용해 IT 제품을 평가함으로써 평가 결과의 호환성이 결여되었던 평가 · 인증 제도의 문제점을 보완하기 위해 각국의 평가기준을 조율하여 개발되었다. CC를 통해 국가 간 평가 결과를 상호인정할 수 있는 기반을 제공하고 중복된 평가로 인한 평가 시간 및 비용을 단축할 수 있는 기반을 제공한다.

본 고에서는 CC 개요 및 CC에서 정의한 평가보증등급을 간략히 소개하고 CC 평가 · 인증 결과를 상호인정하는 국제협정인 CCRA(국제상호인정협정, Common Criteria Recognition Agreement) 동향을 설명한다. 또한, 국내외 IT 제품 평가 · 인증 체계와 연혁 및 IT 제품 평가 · 인증 동향에 대해 알아보기로 한다.



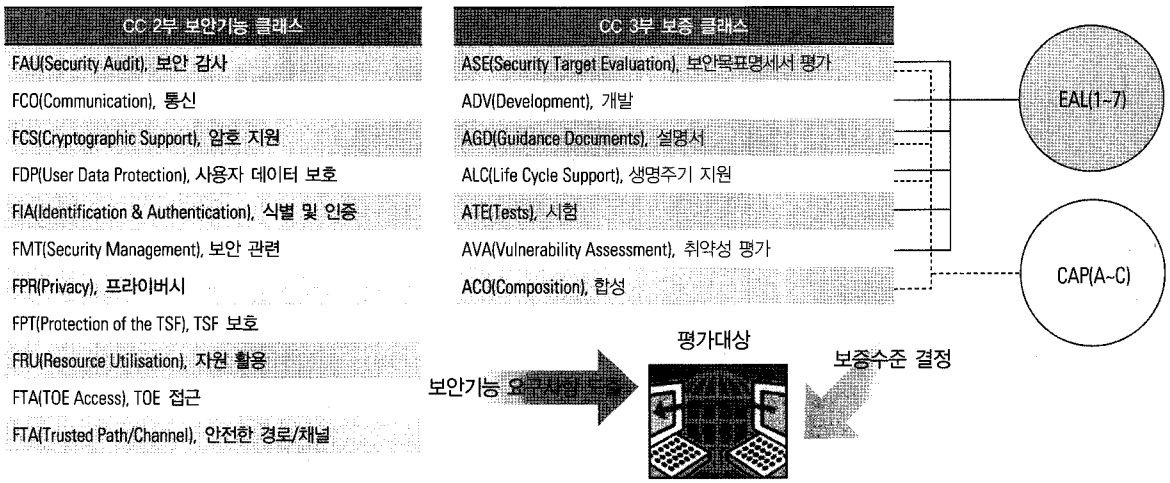
[그림 1] CC 개발 연혁

2. CC 개요

[그림 1]은 CC 개발 연혁을 간략히 보여준다. CC는 미국의 TCSEC 및 Federal Criteria, 유럽의 ITSEC, 캐나다의 CTCPEC을 기반으로 해 1993년 발족된 'CC 프로젝트' 주도 하에 개발되었다. 'CC 프로젝트'는 정보보호제품을 포함하여 IT 제품 시장 확장을 위해 평가결과를 상호인정하기 위한 공통의 평가기준을 개발하고 민간용 정보보호제품의 활성화를 촉진하는 평가 · 인증 제도를 마련하기 위해 일반 사용자의 요구사항을 수용할 수 있는 평가기준을 개발하는 것을 목적으로 하였다. 그 결과 각국에서 활용되고 있던 다양한 평가기준을 단일화하여 공통의 언어와 이해를 기반으로 한 CC를 개발하게 되었고 개발자 및 사용자 등 IT 제품 시장의 요구사항을 반영하여 발전해 왔다.

CC는 3부로 구성되어 있으며 1부는 IT 보안성 평가의 원칙과 일반 개념을 정의하고 CC에 기반을 둔 평가 모델을 제시한다. 2부는 IT 제품의 보안 기능성을 표준화된 방식으로 표현할 수 있는 보안기능 요구사항을 11개의 범주(Class)로 구분해 제공한다. 3부는 IT 제품의 보안 기능성에 대한 신뢰 수준을 측정할 수 있는 보증요구사항을 7개의 범주(Class)로 구분해 제공한다. 또한 3부에서는 보증요구사항의 실현 가능성과 보증에 소요되는 비용을 고려해 미리 정의된 보증 등급을 패키지 형태로 구성하여 제공하며 일반적인 IT 제품 평가에 적용되는 평가보증등급(EAL: Evaluation Assurance Level)을 7단계로 정의하고 기 평가된 IT 컴포넌트와 평가되지 않은 IT 컴포넌트를 합성한 경우 합성 보증수준을 나타내는 합성보증패키지(CAP: Composite Assurance Package)를 3단계로 정의한다.

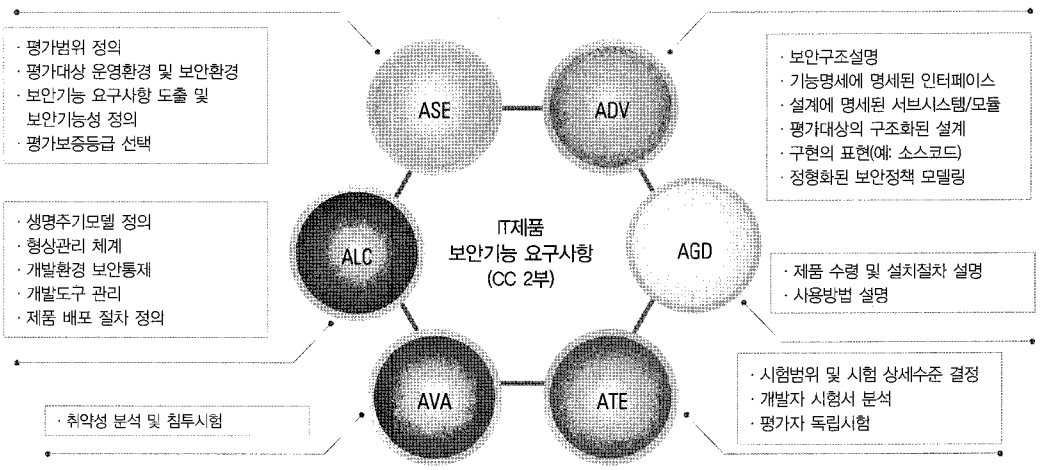
CAP는 CC V3에서 채택된 새로운 보증 수준으로, 현재 공식적으로 CAP에 기반을 두고 평가를 수행하거나 조달 정책에서 CAP로 평가 · 인증된 제품을 요구한다고 발표한 국가는 없다. 그러나 국가별 IT 개발 환경 및 역량 등 현실적 제약으로 인해 IT 제품을 직접 개발하기 보다는 기 개발된 IT 컴포넌트들을 통합(integration)하여 시스템을 구축해 사용하는 국가도 존재하므로 향후 CAP를 적용한 평가 · 인증이 수행될 것으로 예상된다.CC의 EAL은 CAP에만 포함되는 ACO 클래스를 제



[그림 2] CC 개요

외한 6개 클래스 보증요구사항을 범위(Scope), 상세수준(Depth), 엄밀성(Rigour)을 척도로 하여 구성한다. EAL이 높을수록 IT 제품의 더 많은 부분이 포함되고 설계 및 세부적인 구현이 더 정밀하게 전개되며 구조적이고 정형화된 방식을 적용하는 노력을 요구한다. 또한 EAL이 높을수록 IT 제품을 개발 및 유지보수 하는 동안 엄격한 규칙 및 통제 절차가 적용될 것을 요구한다.

CC 평가는 IT 제품에 구현된 보안수단이 보안 위협에 대응하고 조직의 보안정책을 지원하는데 충분함을 입증하는 과정으로써 보안수단은 취약성이 발생할 가능성, 취약성 악용 가능성, 취약성으로 인해 발생하는 피해 등을 감소시킬 수 있도록 채택되어야 한다. 취약성은 일반적으로 IT 제품의 기능과 특성을 나타내는 요구사항 자체의 결함이나 개발 과정에서의 결함, 운영상의 부적절한 관리로 인해 발행할 수 있다. CC 평가는 궁극적으로 이러한 취약성을 제거, 최소화, 탐



[그림 3] CC 보증요구사항 개요

지하기 위한 과정으로써 [그림 3]에서 제시된 각 보증 클래스별 평가 과정을 수행함으로써 IT 제품이 본래 의도한 목적을 만족시킨다는 보증을 얻게 된다.

위와 같이 IT 제품 평가 · 인증 후 발급된 CC 인증서를 국가 간 상호인정하기 위해서는 CC에서 정의한 기준을 공통으로 해석하고 적용하기 위한 방법론이 요구된다. CEM(Common Evaluation Methodology)은 CC 평가 시 CC에 정의된 기준과 평가 증거를 사용하여 평가자가 수행해야 하는 최소 평가행동에 대한 세부 지침을 제공함으로써 CC 평가 결과의 객관성에 기여한다. CEM은 CC가 개정됨에 따라 함께 발전해 왔으며 현재 국제표준(ISO/IEC 18045)으로 지정되어 있다.

3. CC 평가 · 인증 국내외 동향

CC는 2002년 국내 정보보호제품 평가기준으로 채택되었으며 CC 도입 이전에는 침입차단시스템(Firewall)과 침입탐지시스템(IDS)에 한해 각 제품군별로 국내 평가기준을 개발해 적용해 왔다. 국내 평가기준의 경우 신규 제품군을 평가하기 위해서는 해당 제품군에 적용할 수 있는 기준을 우선적으로 개발해야 하는 문제가 있어 평가대상 제품군 확장이 유연하지 못했으나 CC가 적용되면서 전 IT 제품군을 평가할 수 있는 기반을 마련하게 되었다. 2005년 국내 정보보호제품 평가기준을 CC로 단일화하고 2006년 CCRA 인증서 발행국으로 가입하면서 국산 IT 제품의 국제 경쟁력을 강화하고 IT 보안 핵심 기술의 국외 유출을 방지하는 등 국내 CC 평가 · 인증제도를 한 단계 업그레이드하는 계기를 맞게 되었다. 최근에는 네덜란드, 독일, 프랑스 등 유럽 일부 국가만이 보유하고 있었던 IC칩 기반 하드웨어 제품 평가기술을 확보해 전자여권, 스마트카드 등을 평가함으로써 소프트웨어에만 한정되어 있던 국내 CC 평가 분야에 전환점을 가져 왔다.

국내에서 CC에 기반을 두어 평가 · 인증되는 제품군은 과거 침입차단시스템, 침입탐지시스템, 가상사설망 등 네트워크 보안 제품에 한정되어 있었다. 그러나 근래에는 통합보안관리시스템, DB접근통제, 웹방화벽, 바이러스 백신 등 점점 다양화되고 있으며 제품의 형태 또한 단일 제품군에서 여러 제품군이 통합된 복합제품에 대한 평가 신청이 증가하고 있는 추세이다.

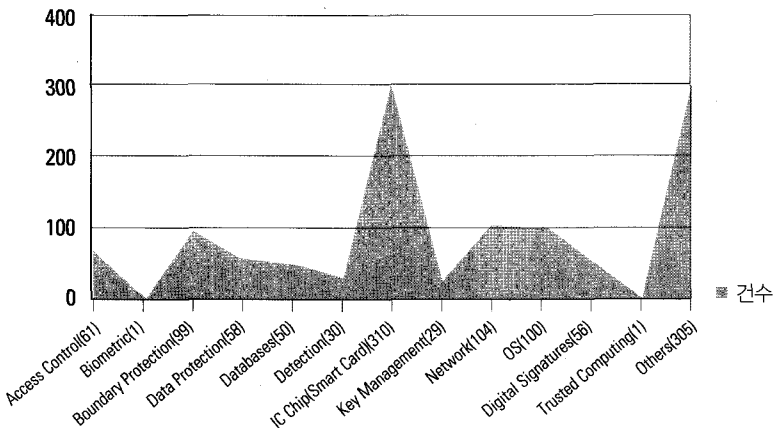
〈표 1〉 국내 평가 · 인증제도 연혁

1995	「정보화촉진기본법 제15조」에 의해 정보보호제품 평가 기반 마련
1998	정보통신망 침입차단시스템 평가기준 고시
2000	정보통신망 침입탐지시스템 평가기준 고시
2002	CC 국내 평가기준 도입
2005	국내 평가기준을 CC로 단일화
2006	정부 · 공공기관 사용 정보보호제품 CC 평가 의무화 CCRA 인증서 발행국 가입
2007	CC 평가 · 인증제도 국제용/국내용으로 이원화 복수 평가기관 제도 도입, 2개 평가기관 추가 지정 (KTL, KOSYAS)
2009	2개 평가기관 추가 지정(TTA, KSEL)

[그림 4]는 CCRA에서 제공하는 CC 평가 · 인증 제품 건수를 제품군별로 분류하여 보여준다. 그림에서 볼 수 있듯이 기존의 IT 제품군 분류 체계에 부합하지 않는 기타 제품군('Others'로 표기) 평가 · 인증이 상당 부분을 차지하고 있으며 국내에서는 아직 평가 경험이 부족한 운영체제나 IC칩 등에 대한 평가 · 인증이 국외에서는 활발하게 이루어지고 있음을 알 수 있다.

국외의 경우에도 국내 CC 평가 환경과 유사하게 변화하고 있으며 급변하는 IT 시장의 요구사항을 수용하고 일관성 있는 평가결과를 유지하기 위해 각국 평가 · 인증기관 간에 기술 및 정책을 교류하고 있다.

평가결과를 상호인정하고 각 평가기관에서 수행된



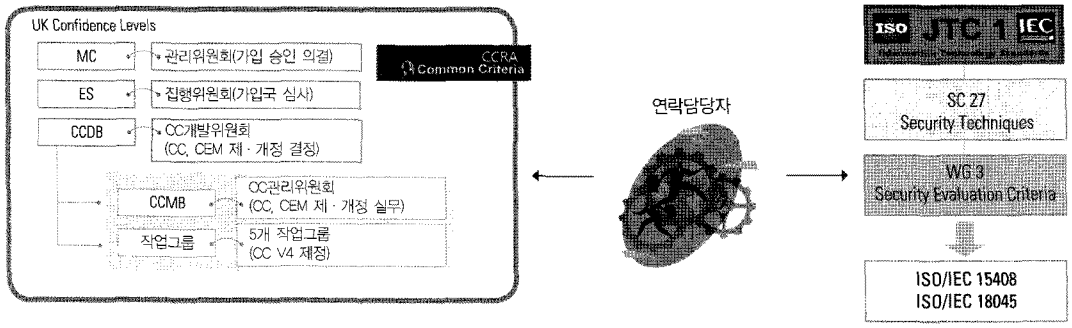
※출처: CC포털 홈페이지(www.commoncriteriaportal.org)

[그림 4] 제품군별 평가 · 인증 현황(CCRA)

CC 평가 결과의 호환성을 높이기 위해서 각국 인증기관은 CC에 적용되는 관리 및 규정 체제인 평가 스킴(Evaluation Scheme)을 확립해 평가의 신뢰도를 검증하고 평가기관과 평가자가 지켜야 하는 규정을 관리 감독한다. CC는 평가 스킴에 대한 요구사항을 다루지 않으며 각국 평가 스킴의 일관성은 CCRA에서 다루어진다. CCRA는 CC에 기반을 둔 IT 제품 평가 · 인증 결과를 상호인정하고 국제적으로 상호 신뢰할 수 있는 평가 환경을 구축하기 위한 국제협정으로, 현재 26개국이 회원국으로 가입되어 있다. CCRA 회원국 자격은 CCRA에서 공인된 평가기관을 보유한 인증서 발행국(CAP: Certificate Authorizing Participants)과, CCRA에서 공인된 평가기관을 보유하지 못해 인증서 발행국에서 발급된 CC 인증서를 자국에서 인정해 주기만 하는 인증서 수용국(CCP: Certificate Consuming Participants)으로 이원화되어 있으며, 한국은 2006년 인증서 발행국으로 CCRA에 가입했다. 현재 CCRA에서는 일부 고등급 요구사항에 대하여 회원국 전체가 합의한 공통의 평가방법론을 도출하지 못해 EAL4 등급까지 상호인정하고 있다.

CC 및 CEM은 CCRA에서 상호인정의 기반이 되는 기술문서이자 ISO 국제표준이므로 문서의 제 · 개정 또한 CCRA와 ISO에서 공동으로 담당하고 있으며 CCRA에서 주로 제 · 개정 실무를 담당하고 연락담당자를 통하여 ISO 회원국의 의견을 수렴하고 있다.

CCRA가 출범한 이래 CC는 사용자, 개발자, 평가자, 인증자 등 다양한 관계자의 요구사항을 반영하여 개정되어 왔으며 현재 CC V3.1이 최신 기준으로써 평가에 적용되고 있다. 동시에 CCRA는 급변하는 시장 논리 속에서 CC 기반 평가제도의 존속 및 발전을 위해 현재 5개 작업그룹을 구성해 CC V4개발을 위한 연구 활동을 수행하고 있다. CCRA 작업그룹에서는 IT 제품의 취약성을 찾기 위한 평가 활동을 보강하기 위해 평가 시 보증 수준을 만족하기 위한 수단 및 프로세스를 개발한다. 또한 평가 · 인증된 제품이 변경된 경우 적시에 관리될 수 있도록 개발자의 제품 개발 및 유지보수 능력을 심사하는 프로세스를 연구하며 평가 효율성을 제고하기 위한 프로세스 개선 방안을 마련하는 등 현재 CC 평가 · 인증 방법론의 문제점을 개선하기 위한 활동을 수행하고 있다.



[그림 5] CC 제 · 개정 관련 기구

4. 맺음말

CC는 IT 보안 기능성에 직접적으로 관련된 거의 모든 보안 수단을 다룬다. 사용자는 CC를 사용하여 자신이 원하는 IT 제품에 대한 요구사항을 제시하고 평가 · 인증된 제품 목록으로부터 자신들의 보안 요구를 만족하는 IT 제품을 선별해 사용할 수 있으며, 개발자는 자신이 개발한 IT 제품이 사용자의 요구에 부합한다는 근거를 제시하기 위해 평가에 필요한 증거를 산출할 때 CC를 활용할 수 있다. 평가자는 개발자의 IT 제품이 사용자의 요구에 부합함을 객관적으로 확인하고 검증하기 위해 CC를 사용할 것이다.

CC 평가 체계는 평가대상이 되는 IT 제품의 유형이나 구현 형태에 제약을 두지 않으며 현존하는 IT 기술에만 국한된 평가기준이 아니라 신규로 개발되는 IT 기술에까지 확장될 수 있는 유연한 체계로써 IT 보증 분야에서 활용도 및 시장성이 가장 높은 분야라 할 수 있다.

현재까지 CC는 성공적으로 광범위하게 국제적으로 인정받아 왔으며, IT 시장의 급격한 진화에 부응하기 위해 성장화고 변화해 왔다. 최근 국내에서도 다양한 유형의 IT 제품이 CC에 기반을 두어 평가 · 인증되고 있으나 운영체제, DBMS, IC칩, PKI 시스템 등 아직 평가경험이 부족하거나 평가를 시도하지 않은 분야가 많이 존재한다. 유럽의 경우 전자결재 단말기, 전자투표기, 택시미터기 등 신규 IT 영역으로까지 CC 평가를 확장하고 있는 추세임을 감안한다면 국내의 CC 평가 영역도 잠재력이 무한할 것으로 판단된다.

[참고문헌]

[1] CCMB-2009-07-001~003, Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3, CCMB, 2009. 7.

[2] CCMB-2009-07-004, Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3, CCMB, 2009. 7.

[3] 정보보호제품 평가 · 인증 교육 일반과정 '평가인증 제도 소개', IT보안인증사무국, 2009.03.