# 정보보호시스템 공통평가기준 기술동향

**The Technology Trend of Common Criteria for Information Security System**

김광식(K.S. Kim) 네트워크보안구조연구팀 계약직 선임연구원
남택용(T.Y. Nam) 네트워크보안구조연구팀 선임연구원, 팀장

이제 공통평가기준(CC)의 도입은 거를 수 없는 대세로 자리 잡고 있으며, 국내에서도 CC를 도입하기 위해 인증기관과 평가기관들이 도입을 위한 준비를 서두르고 있으나 개발자 입장에서는 아직 미흡한 실정이다. 따라서, 본 고에서는 CC를 고려하여 정보보호시스템을 개발하고자 하는 연구기관 및 업체에서 개발전략을 수립하는 데 도움이 될 수 있는 CC 관련 기술동향을 살펴보았다. 먼저, 기존 정보보호시스템 평가기준인 TCSEC과 ITSEC에 대해 간략히 살펴본 후, 국제간에 상호 인증을 받을 수 있는 정보보호시스템 공통평가기준에 대해 CC 출현 배경, CC 표준 규격, PP와 ST 개발동향, CC의 최근 표준화동향 관점에서 살펴본다. 그리고, 연구개발을 추진하는 개발자 입장에서 연구개발체계에 CC를 어떻게 적용할 것인가에 대한 방안을 제시한다. 이를 위해 먼저, CC 관련 주요 이슈에 대해 ICCC'2002를 통해 알게 된 내용을 위주로 살펴보고, 연구개발체계에 CC 도입시 개발자들이 고려해야 할 개발 보증 증거물들에 대해 살펴본다.

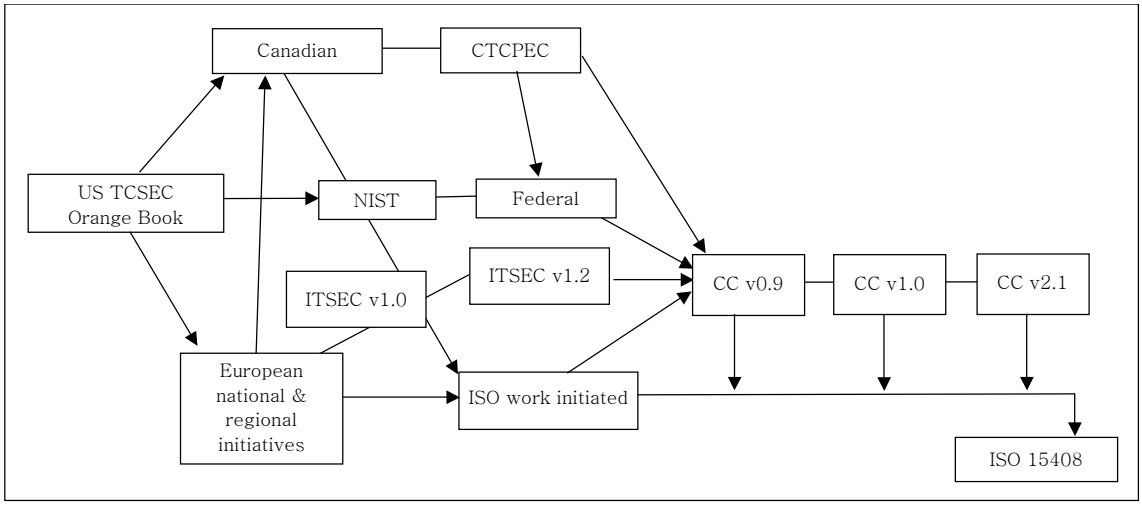
## I. 서 론

1980년 초반에 TCSEC(Trusted Computer System Evaluation Criteria)은 미국에서 평가기준 중 처음으로 개발되었다. 그 다음 10년 동안 여러 나라에서 TCSEC의 개념을 기본으로 하되 일반적으로 IT(Information Technology)의 진화하는 본질에 보다 더 유연하고 융통성이 있는 평가기준을 개발하기 위한 주도권 싸움을 시작했다.

유럽에서는 프랑스, 독일, 네덜란드 및 영국이 참여한 공동 개발 후에 EC(유럽연합)에 의해 1991년에 TCSEC의 개념을 기반으로 ITSEC(Information Technology Security Evaluation Criteria) version 1.2가 개발되었다. ITSEC은 환경을 고려하여 보안기능을 설정하는 것 외에 TCSEC 혹은 독일의 ZSIEC(Criteria for the evaluation of trustworthiness of information technology systems)에서 미리 정의한 보안기능을 사용토록 하였으며, 제품에 대한 평가는 CC(Common Criteria)와 같이 보증부분만 가지고 수행이 된다.

캐나다에서는 ITSEC과 TCSEC 접근법의 조합으로서 CTCPEC(Canadian Trusted Computer Product Evaluation Criteria) version 3.0이 1993년 초에 출판되었다. 미국에서는 평가기준을 위한 미국과 유럽의 개념을 조합하는 두번째 접근법으로서 FC(Federal Criteria) version 1.0 초안이 또한 1993년 초에 출판되었다.

1993년 6월, CTCPEC, FC, TCSEC과 ITSEC을 개발한 각 국가의 평가기관들은 각 국가적으로 독립된 평가 기준을 통합하고자 하는 프로젝트를 시작하였으며, 이를 CC 프로젝트라 하였다. CC 프로젝트는 기존의 평가 기준들간의 기술적/개념적 차이를 통




(그림 1) CC 발전 경로

<표 1> CCRA 서명 국가별 관련 기관 및 홈페이지

| 국가 | 기관/홈페이지 |
|---|---|
| 호주와 뉴질랜드 | AISEP(Australasion Information Security Evaluation Programme)<br>- 홈페이지: http://www.dsd.gov.au/infosec |
| 캐나다 | CSE(Communications Security Establishment)<br>- 홈페이지: http://www.cse-cst.gc.ca/en/services/common_criteria/ |
| 핀란드 | Ministry of Finance |
| 프랑스 | DCSSI(Direction Centrale de la Securite des Systemes d'Information)<br>- 홈페이지: http://www.ssi.gouv.fr |
| 독일 | BSI(Bundesant fur Sicherheit in der Informationstechnik)<br>- 홈페이지: http://www.bsi.de/cc |
| 그리스 | Ministry of Interior |
| 이스라엘 | Standards Institution of Israel |
| 이태리 | Autorità Nazionale per la Sicurezza |
| 네덜란드 | NLNCSA(Netherlands National Communications Security Agency)<br>- 홈페이지: http://www.commoncriteria.nl |
| 노르웨이 | CHOD Norway/Security Division |
| 스페인 | Ministerio de Administraciones Publicas |
| 영국 | CESG(Communication Electronics Security Group)<br>- 홈페이지: http://www.cesg.gov.uk/assurance/iacs/itsec/index.htm |
| 미국 | NIST(National Institute of Standards and Technology)<br>NSA(National Security Agency)<br>NIAP(National Information Assurance Partnership)<br>- 홈페이지: http://niap.nist.gov/cc-scheme<br>- 홈페이지: http://www.commoncriteria.org |

합하여 국제 표준화를 만들자는 목표로 추진되었으며, 1996년 1월에 CC version 1.0, 1997년 10월에 version 2.0, 1999년 8월에 ISO 15408/version 2.1이 완성되었고, 2003년 4월쯤 version 3.0이 만들어질 예정으로 있다[1]. CC에 대한 발전 경로는 (그림 1)과 같다.

2년간의 격렬한 협상 끝에 1998년 10월에 미국, 캐나다, 프랑스, 독일 및 영국의 정보조직들은 CC 기반 평가를 위한 역사적인 상호인증협정(Common Criteria Recognition Arrangement: CCRA)에 서명했다. 이 협정의 취지는 CC 증명을 받는 IT 제품과 보호프로파일들이 다시 평가되고 증명/확인 받을 필요 없이 획득되거나 사용될 수 있는 상황을 만들어냄으로써 이러한 목적들을 진보시키는 것이다. 현재 이 협정에 서명한 국가는 <표 1>과 같다.

## II. 기존 정보보호시스템 평가기준 동향

### 1. TCSEC

TCSEC 평가 기준은 미국의 정보보호시스템 평가 표준으로 채택되었고 세계 최초의 보안 시스템 평가 기준으로 다른 평가 기준의 모체가 되었다. TCSEC에서 각 보안 등급을 평가하기 위해 크게 네 가지 범주에 해당되는 요구사항을 가지고 있으며, 각각 보안정책, 책임성, 보증, 문서화 등이다. 그리고, TCSEC 평가 기준의 보안 등급을 받기 위해서는 네 가지 범주에서 지정해주는 요구사항들을 만족시켜 주어야 하며, 어느 정도 수준을 만족시키는지에 따라서 크게 D, C, B, A의 4가지의 평가 등급 중 하나에 속하게 된다[2].

TCSEC의 평가 요구사항은 보안정책, 책임성, 보증, 문서화 사항들로 구성되며, 각각은 다음과 같은 세부적인 상세 보안 요구사항으로 나누어진다.

보안정책은 정보를 보호하려는 조직을 위한 기본적인 요구사항으로 임의적 접근 제어(Discretionary Access Control: DAC), 강제적 접근제어(Mandatory Access Control: MAC), 레이블, 레이블된 정보의 유출, 사람이 읽을 수 있는 출력형태로 레이블, 장치 레이블 등이 있다.

책임성은 시스템이 DAC와 MAC를 지원하기 위한 기능으로 식별 및 인증, 감사 및 신뢰성 있는 경로 기능 등을 제공한다.

보증은 시스템의 보안기능이 올바르게 작동하는가를 검사하여 시스템의 신뢰성을 제공하는 요구사항으로 시스템 구조, 시스템의 무결성, 시스템시험, 설계 명세서 및 검증, 형상관리, 비밀 채널의 분석 등이 있다.

<표 2> TCSEC의 등급별 평가기준

| 등급 | 설명 |
|---|---|
| D | 최소한의 보호(minimal) |
| C1 | 임의적 정보보호(discretionary) |
| C2 | 통제된 접근보호(controlled access) |
| B1 | 레이블된 정보보호(labeled security) |
| B2 | 계층 구조화된 정보보호(structured ) |
| B3 | 보안영역(security domain) |
| A1 | 검증된 보호(verified design) |

문서화는 매우 어렵고 시간이 많이 걸리는 작업이지만, 평가를 위해 꼭 필요한 작업이며 문서에는 사용자를 위한 보안 지침서, 관리자를 위한 보안 특성 지침서, 시험문서, 설계문서 등이 있다.

TCSEC은 <표 2>와 같이 크게 D, C, B, A의 네 등급으로 분류할 수 있으며, 세부적으로는 D, C1, C2, B1, B2, B3, A1의 등급으로 나눌 수 있다. 여기서 A 등급은 가장 높은 보안 등급을 나타내며, D 등급은 보안이 가장 낮다. TCSEC에서 D 등급은 보안에 대한 요구사항이 없는 최소한의 보안 등급을 의미하고, C1/C2/B1 등급은 상업적으로 사용되는 많은 운영체제에서 요구하는 보안 특성을 기술하고 있으며, B2 등급은 운영체제의 설계 단계에서부터 보안 요구사항을 반영하게 된다. 마지막으로 B3/A1 등급은 TCB에 대한 정형적인 검증을 요구한다. TCSEC의 등급체계는 높은 등급으로 갈수록 보안기능요구사항과 보안보증요구사항이 체계적으로 증가한다.

### 2. ITSEC

TCSEC은 미국에서 개발되었지만, 유럽의 정보보호 시스템을 평가하는 데 역시 사용되었다. 유럽 몇몇 국가들은 정보보호시스템 평가기준 및 방법에 대한 필요성을 느끼게 되었고, 여러 유럽 국가들의

노력에 의해서 ITSEC이 탄생되었다. ITSEC의 개발 과정을 살펴보면, 영국, 독일 그리고 프랑스의 세 국가가 거의 같은 시기에 서로 독립적으로 평가 기준 작업에 돌입하였으며, 1989년 영국과 독일이 최초 초안을 발표하게 되었다. 이후, ITSEC은 영국, 독일, 프랑스 및 네덜란드 등 자국의 정보보호시스템 평가기준을 제정하여 시행하던 4개국이 평가제품의 상호 인정 및 평가기준이 상이함에 따른 정보보호 제품의 평가에 소요되는 시간, 인력 및 소요 비용을 절감하기 위하여 1991년에 ITSEC v1.2를 제정하였다[2].

ITSEC은 TCSEC과는 달리 단일 기준으로 모든 정보보호제품을 평가하고자 하였다. 따라서 보안기능은 개발자가 제품이 사용될 환경을 고려하여 보안기능을 설정하거나 TCSEC 혹은 독일의 ZSIEC에서 미리 정의한 보안기능을 사용토록 하였으며 제품에 대한 평가는 보증부분만 가지고 수행이 된다.

기능에 의한 기준으로 보안정책은 어떻게 보안시스템이 필요한 정보를 관리하고, 보호하는 것인가에 대해 기술하고, 제품의 이론적 근거는 상품이 시스템 보안 목적을 만족시키는 데 도움을 줄 것인가에 대한 정보를 제공한다.

마지막으로 보안 강화 기능요구사항은 보안정책을 만족시키는 미리 정의된 기능 클래스(신분확인 및 접근제어 등)를 이용하거나, 보안 기능을 정의한 표준을 이용한다. 보증 효과는 보안 강화 기능과 방법이 언급된 보안 목표를 실제로 만족시킬 수 있는지를 평가하는 수단이고 요구사항은 대체로 구축과 운영의 효용성에 대한 문서를 요구한다. 그리고, 보증 정확성은 보안 강화 기능과 방법이 실제로 올바르게 구현되었는지를 평가한다.

기능에 의한 등급으로 TCSEC 호환 등급은 F-C1(C1), F-C2(C2), F-B1(B1), F-B2(B2), F-B3(B3~A1)이고 그 외에 F-IN(무결성 강화), F-AV(가용성 강화), F-DI(교환자료의 무결성 강화), F-DC(교환자료의 비밀성 강화), F-DX(교환자료의 비밀성과 무결성 강화)가 있다.

# III. 정보보호시스템 공통평가기준 동향

## 1. CC 출현 배경

공통평가기준(CC)은 국제 사회 내에 널리 사용되는 IT 보안의 평가기준을 개발하기 위한 일련의 노력의 산출물이다. 정보보호시스템의 공통 평가 기준으로 현재 널리 사용되는 국제 공통평가 기준인 CC는 정보보호시스템의 보안 기능요구사항과 이를 평가하는 동안 적용하는 보증요구사항에 대한 공통의 집합을 정하여 서로 독립적으로 수행한 평가 결과들을 호환할 수 있도록 하기 위한 것이다. CC에서는 EAL(Evaluation Assurance Level) 1 ~ EAL 7까지 보증등급은 있으나, TCSEC과는 달리 보안기능에 대한 등급은 없는 것이 특징이다. 보안기능은 ITSEC과 같이 개발자가 제품이 사용될 환경을 고려하여 보안기능을 설정하도록 되어 있으며, 제품에 대한 평가는 보증부분만 가지고 수행이 된다.

CC는 보증등급을 평가하므로 해서, 평가기관에서 보호프로파일(Protection Profile: PP)이나 보안목표명세서(Security Target: ST)를 평가할 때, PP에 포함된 보안목적, 보안기능요구사항, 보안보증요구사항 그 자체를 평가하지는 않는다. 그들 간의 일치성을 평가할 뿐이다. 이 점이 기존의 TCSEC과 다른 점이다. 그래서, 보안 보증등급인 EAL 등급이 높다고 해서, 보안 기능이 강화된 것이라고 할 수 없다. 오히려, 정형적으로 모델링 될 수 있는 위험요소는 더 높은 EAL 등급을 받을 수 있다. 정형적인 모델링이 되지 않는 위험요소는 더 낮은 EAL 등급을 받게 되지만, 이를 고려한 제품은 보안 기능이 더 강하다고 할 수 있다.

## 2. CC 표준 규격

IT 보안 평가를 위한 CC는 ISO/IEC 15408: “Evaluation criteria for information technology security”에 표준 문서로 명시되어 있으며, 모든 정보보호시스템 유형을 포괄할 수 있는 보안 평가 기준을 제시하고 있다[1]. CC는 아래와 같이 구별되는

<표 3> CC의 파트와 사용자 그룹과의 관계

| | 고객 | 개발자 | 평가자 |
|---|---|---|---|
| Part 1: 소개와 일반적 모델 | 배경 정보와 참고 목적을 위한 사용<br>PP를 위한 가이드 구조 | 요구사항 개발과 TOE를 위한 보안 규격을 공식화하기 위한 배경정보와 참고를 위한 사용 | 배경 정보와 참고 목적을 위한 사용<br>PP와 ST를 위한 가이드구조 |
| Part 2: 보안기능 요구사항 | 보안 기능을 위한 요구사항 진술을 공식화할 때 가이드와 참고를 위한 사용 | 기능요구사항의 진술을 해석하고 TOE를 위한 기능 규격을 공식화할 때 참고를 위한 사용 | TOE가 주장하는 기능이 있는지 여부를 결정할 때 평가기준의 필수 진술로서 사용 |
| Part 3: 보안보증 요구사항 | 보증의 요구레벨을 결정할 때 가이드를 위한 사용 | 보증요구사항의 진술 해석과 TOE를 위한 보증 접근법을 결정할 때 참고를 위한 사용 | TOE의 보증을 결정할 때와 PP와 ST를 평가할 때 평가기준의 필수 진술로서 사용 |

그러나 관련이 있는 부분들의 세트로 소개된다. CC에서 사용되는 항목들은 Part 1에 설명되어 있다.

Part 1(개요와 일반적 모델)은 CC의 소개 부분이다. 이 부분은 IT 보안 평가의 일반적인 개념과 원칙을 정의하고 일반적인 평가모델을 소개한다. Part 1은 또한 IT 보안요구사항의 선택과 정의를 위하여, 그리고 제품과 시스템을 위한 상위수준 규격을 작성하기 위하여 IT 보안 목적을 표현하기 위한 구성요소를 소개한다. 게다가, CC의 각 파트의 유용성은 목표 청중 각각의 항목으로 설명된다.

Part 2(보안 기능요구사항)는 평가목표물(Target of Evaluation: TOE)을 위한 보안 기능요구사항을 표현하는 표준화된 방법으로서 보안 기능 컴포넌트 세트를 포함하고 있다. Part 2는 기능 컴포넌트, 패밀리 및 클래스의 세트로 분류하고 있다.

Part 3(보안 보증요구사항)는 TOE를 위한 보증 요구사항을 표현하는 표준화된 방법으로서 보증 컴포넌트 세트를 포함하고 있다. Part 3는 보증 컴포넌트, 패밀리 및 클래스의 세트로 분류하고 있다. Part 3는 또한 PP와 ST를 위한 평가기준을 정의하고 EAL이라 불리는 TOE를 위한 보증등급을 위한 선정의된 CC 척도를 정의하는 평가보증레벨을 포함하고 있다.

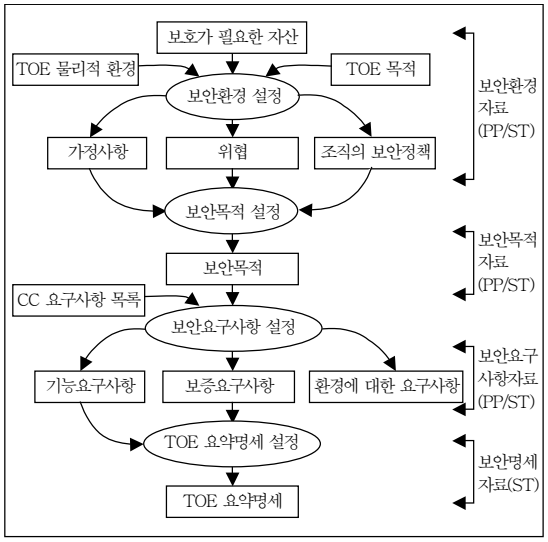
상기의 열거된 3개 파트로 구성된 CC의 지원을 위하여 기술적인 원리 자료와 가이드 문서들을 포함하는 다른 형태의 문서들이 출판될 것으로 기대된다. <표 3>은 CC의 파트들이 3개 주요 CC 사용자 그룹들에게 어떻게 흥미를 주는지를 보여준다.

보증등급 중 EAL 1은 입문 수준이다. EAL 4까지 등급이 높아질수록 엄격함과 상세함이 증가되지만 굉장히 특수화된 보안 엔지니어링 기술의 도입을 필요로 하지는 않는다. EAL 4는 일반적으로 평가를 염두에 두고 개발되지 않은 제품과 시스템에 적용가능 할 수 있다.

EAL 4급 이상은 등급이 높아질수록 특수화된 보안 엔지니어링 기술이 증가되어 적용되어야 한다. 이 보증레벨의 요구사항을 만족하는 TOE는 아마도 그 목적과 함께 설계되고 개발될 것이다. 최고 레벨(EAL 7)에서 요구사항을 만족하는 제품의 구현 가능성에 대해서는 한계가 많다. 그 이유는 부분적으로는 개발자와 평가자의 활동에 상당한 비용의 영향 때문에 그리고 가장 단순한 제품과 다른 어떠한 제품들은 공식적인 분석을 위한 최신 기술들을 제시하는 것이 너무 난해하기 때문이다.

## 3. 보호프로파일과 보안목표명세서

CC는 보호프로파일(PP) 혹은 보안목표명세서(ST)라는 별도의 산출물을 통해 개별 정보보호시스템의 평가에 적용된다. PP는 정보보호시스템의 보안 요구사항들로 완성한 독립 집합체로서 사용자, 개발자, 기타 사람들이 PP를 개발할 수 있다. ISO/IEC PDTR(Proposed Draft Technical Report) 15446은 공식적인 표준 문서는 아니지만 PP, ST의 작성을 위한 가이드라인을 제시하고 있으며, 아주 유용한 문서이다[3]. 이 문서에서는 PP와 ST의 세부 절들에 대한 전체적인 설명과 각 절의 생성방법




(그림 2) PP와 ST 도출 방법

및 항목에 대한 가이드를 제시하고 있으며, 어떻게 패키지를 규정하는지에 대해 설명하고 있다. 또한 환경과 위험 요소에 대한 일반적으로 사용 가능한 예제를 포함하고 있다. (그림 2)는 PP와 ST의 도출 방법에 대하여 보여준다. 자세한 사항은 ISO/IEC PDTR 15446을 참고하면 된다.

PP와 ST를 작성하는 데 도움을 주는 CC 툴박스(toolbox)는 PP와 ST의 개발에 대한 공통기준의 적용을 용이하게 하기 위해 미국의 NIST와 NSA가 공동으로 설립한 NIAP에 의해 개발된 소프트웨어 패키지로서, PP와 ST 작성을 위해 인터뷰 형식을 취하고 있는 것이 특징이며, 기존 PP와 ST의 툴박스 파일을 사용하여, 새로운 PP와 ST를 손쉽게 작성 가능하다[4]. PP와 ST를 작성하는 데 도움을 주는 CC 툴박스가 참조로 하는 데이터베이스인 CC PKB(Profiling Knowledge Base)는 CC 툴박스를 위해 만들어졌는데, PP와 ST 작성 및 다양한 종류의 정보들 간의 논리적인 관계성을 추적하기 위해 필요한 여러 종류의 정보들을 포함하도록 설계되어 있다. 이 데이터베이스의 설계는 CC 툴박스 요구사항과 PP를 위한 CC 요구사항 모두에 의해 영향을 받았다. CC PKB는 CC 툴박스를 이용하여 PP와 ST를 작성할 때 필요한 사항들을 참고하는 데이터베이스로서, MS Access 97, 2000으로 구현되어 있다. PP의 모든 부분을 위한 데이터베이스는 아니지만 보안 환경과 이론적 근거까지 상당부분에 대해 참조가 가능하다.

2002년 7월 현재, CC 홈페이지(www.commoncriteria.org)에 등록되었거나, 등록중인 PP는 아래와 같다. PP의 종류는 크게 7개 분야 즉, 데이터베이스, 통신, 네트워킹, OS, 스마트카드, 접근제어 및 기타 분야로 나눌 수 있다(<표 4> 참조).

본 고에서는 CC 홈페이지에 있는 PP만 소개했으나, 세계 각국에서 개발된 보호프로파일에 대한 자세한 사항은 제7회 정보보호심포지엄 SIS 2002 (2002.7.9.~10.)의 학술회의지의 314~315 페이지에 자세히 나와 있으므로 참고하면 된다[5].

2002년 6월까지 CC 홈페이지에 등록된 제품은 크게 7개 분야로 데이터베이스 분야 5개, 통신분야 3개, 네트워킹 분야 25개, OS 분야 4개, 스마트카드 분야 3개, 접근제어 분야 6개, 기타 분야 6개로 구성되어 있다(<표 5> 참조).

CC 홈페이지에 평가중인 제품에 대한 리스트는 7개 분야에 걸쳐 아래와 같다(<표 6> 참조).

본 고에서는 CC 홈페이지에 있는 제품만 소개했으나, 세계 각국에서 개발된 제품들에 대한 자세한 사항은 <표 1> CCRA 서명 국가별 관련 기관들의 홈페이지를 보면 자세히 나와 있으므로 참고하면 된다.

## 4. CC의 최근 표준화동향

1999년 8월에 작성된 CC version 2.1 및 CEM (Common Evaluation Methodology) 1.0이 작성된 이후 아직 공식적인 개정은 없으나, 보완(supplement) 문서들이 만들어지고 있다. 그 중에 하나는 2002년 2월에 작성된 보완 문서인 ALC_ FLR - Flaw Remediation version 1.1이다[6],[7]. 1999년 8월에 발표된 CEM Part 2, v1.0은 CC v2.1에 정의된 대로 EAL 1부터 4까지를 위한 보증 컴포넌트를 적용할 때 사용되는 방법론을 서술하고 있다[8]. 그러나, CEM은 APE(PP evaluation)와 ASE(ST

<표 4> CC 홈페이지에 있는 PP 리스트

| 입력 레이블 | 제목 | 보증등급 | 공급자 | 상태 |
|---|---|---|---|---|
| PP-001 | Directory for US Department of Defense Class 4 PKI PP | EAL3 | National Security Agency | 인증됨 |
| PP-002 | Trusted Platform Module(TPM) Protection Profile | EAL2 | Trusted Computing Platform Alliance(TCPA) | 개발중 |
| PP-003 | Passport Certificate Server | EAL2+ | Diversinet Corp. | 초안 |
| PP-004 | Role-Based Access Control Protection Profile Version 1.0 | EAL2 | National Institute of Standards and Technologies | 인증됨 |
| PP-005 | Traffic Filter Firewall Protection Profile For Medium Robustness Environments | EAL2+ | National Security Agency | 인증됨 |
| PP-006 | Certificate Issuing and Management Components | EAL4 | Sponsor: National Security Agency | 인증됨 |
| PP-007 | Labeled Security Protection Profile Version 1.b | EAL3 | National Security Agency | 인증됨 |
| PP-008 | Oracle DBMS Protection Profile | EAL3 | Oracle Corporation | 인증됨 |
| PP-009 | Role-Based Access Control Protection Profile Version 1.0 | EAL2 | National Institute of Standards and Technology | 인증됨 |
| PP-010 | Traffic Filter Firewall Protection Profile for Low Risk Environments(Version1.1) | EAL2 | National Security Agency | 인증됨 |
| PP-011 | Application Level Firewall Protection Profile for Low Risk Environments(Version1.d) | EAL2 | National Security Agency | 초안 |
| PP-012 | Controlled Access Protection Profile | EAL3 | National Security Agency | 인증됨 |
| PP-013 | Postage Meter Approval Protection Profile | EAL2+ | Consignia | 인증됨 |
| PP-014 | Privilege Directed Content Protection Profile | EAL2 | Authorizor Ltd. | 인증됨 |
| PP-015 | Application-level Firewall Protection Profile For Medium Robustness Environments | EAL2+ | National Security Agency | 인증됨 |
| PP-016 | U.S. Department of Defense Biometrics Office, Biometric System. Protection Profile For Medium Robustness Environments, Version 0.01 | EAL4 | DoD Biometrics Management Office(DoD BMO) | 초안 |
| PP-017 | Intrusion Detection System Analyzer -Draft 3 | EAL2 | National Security Agency | 초안 |
| PP-018 | Intrusion Detection System Sensor - Draft 3 | EAL2 | National Security Agency | 초안 |
| PP-019 | Key Recovery for Third Party Requestors Version 1.0 | EAL3 | National Security Agency | 초안 |
| PP-020 | Key Recovery for Agent Systems Version 1.1 | EAL3 | National Security Agency | 초안 |
| PP-021 | Key Recovery for End Systems Version 2 | EAL1 | National Security Agency | 초안 |
| PP-022 | Protection Profile for Multilevel OS - Requiring Medium Robustness | EAL4+ | National Security Agency | 인증됨 |
| PP-023 | Peer-to-Peer Wireless Local Area Network(WLAN) for Sensitive But Unclassified Environments - Version 0.6 | EAL3 | Boozllen & Hamilton, National Security, Tresys Technology | 초안 |
| PP-024 | Protection Profile for Switches and Routers | EAL3 | National Security Agency | 초안 |
| PP-025 | Single-level OS's in Environments Requiring Medium PP | EAL4+ | National Security Agency | 인증됨 |
| PP-026 | A Goal VPN Protection Profile For Protecting Sensitive Information - Version 2.0 | EAL3 | National Security Agency | 초안 |
| PP-027 | Infrastructure Wireless Local Area Network(WLAN) For Sensitive But Unclassified Environments | EAL3 | Boozllen & Hamilton and Tresys Technology | 초안 |
| PP-028 | Smart Card Protection Profile | EAL4+ | SCSUG | 인증됨 |
| PP-029 | The PKI Secure Kernel Protection Profile | EAL4 | PKI PP Working Group | 인증됨 |
| PP-030 | Oracle Government Database Management System | EAL3 | Oracle Corporation | 인증됨 |

<표 5> CC 홈페이지에 있는 인증 제품 리스트

| 번호 | 제품 | 보증등급 | 공급자 | 인증시점 |
|---|---|---|---|---|
| 1 | Oracle 8 Release 8.0.5 | EAL4 | Oracle Corporation | 2000/10 |
| 2 | Oracle 8 Release 8.1.7 | EAL4 | Oracle Corporation | 2001/07 |
| 3 | Oracle Government Database Management System Protection Profile | EAL3 | Oracle Corporation | 1998/10 |
| 4 | Oracle Commercial Database Management System Protection Profile | EAL3 | Oracle Corporation | 1998/09 |
| 5 | Oracle 7 Release 7.2.2.4.13 | EAL4 | Oracle Corporation | 1998/09 |
| 6 | Entrust RA and Entrust/Authority from Entrust/PKI 5.1 | EAL3 | Entrust Technologies Limited | 2001/02 |
| 7 | Entrust/RA and Entrust/Authority from Entrust/PKI 5.0 | EAL3 | Entrust Technologies Limited | 2000/03 |
| 8 | Entrust/PKI 4.0a | EAL3 | Entrust Technologies Limited | 2000/01 |
| 9 | Secure Session VPN Version 4.1 | EAL1 | KyberPASS Corporation and XCP Security Systems PtyLtd . | 2000/01 |
| 10 | SecureLogix Corporation?Enterprise Telephony Management ETM?Platform Version 3.0.1 for Microsoft? 2000/NT4, and Sun Microsystems Inc. Solaris?7/8 | EAL2+ | SecureLogix Corporation | 2002/02 |
| 11 | BorderWare Version 6.1.1 Firewall Server | EAL4 | BorderWare Technologies Inc . | 2000/01 |
| 12 | SecureSwitch Dual Network Switch, Model #5000600 | EAL4 | Market Central, Inc. | 2001/10 |
| 13 | WatchGuard LiveSecurity System with Firebox II 4.1 | EAL2 | WatchGuard Technologies | 2000/10 |
| 14 | Lucent Managed Firewall - Version 3.0(Build 150) | EAL2 | Lucent Technologies | 1999/01 |
| 15 | Check Point FireWall-1 Version 4.0(SP 5) | EAL2 | Check Point Software Technologies, Inc. | 1999/10 |
| 16 | Lucent Managed Firewall - Version 4.0(Build 199) | EAL2 | Lucent Technologies | 2000/02 |
| 17 | VCS Firewall Version 3.0 | EAL1 | The Knowledge Group | 1999/03 |
| 18 | Symantec Enterprise Firewall Version 7.0 | EAL4 | Symantec | 2002/05 |
| 19 | CTAM Cyphercell ATM Data Encryptor Version 1.2.1 and Cyphermanager Version 3.2.0 | EAL4 | CTAM Pty Ltd. | 2001/04 |
| 20 | Milkyway Networks Black Hole Firewall Version 3.01E2 for SPARCstations(SecurIT) | EAL3 | SLM(Milkyway) Networks Corporation | 1997/08 |
| 21 | Gauntlet Internet Firewall 6.0 on Sun Solaris | EAL4 | Secure Computing Corporation | 2002/04 |
| 22 | SecureDoc | EAL1 | WinMagic, Inc. | 1999/07 |
| 23 | Dragonfly Guard Model G.12 Software Release 3.0 | EAL2 | ITT Industries | 1998/10 |
| 24 | Dragonfly Companion Version 3.02 | EAL2 | ITT Industries | 1998/10 |
| 25 | SuperNet 2000 | EAL4 | Electronic Engineering Systems, Inc. (EESI) | 2000/10 |
| 26 | Tumbleweed Messaging Management System - Version: 4.6 | EAL2 | Tumbleweed Communications Pty. Ltd. | 2002/03 |
| 27 | Conseal Private Desktop Firewall | EAL1 | Signal 9 Solutions | 1999/05 |
| 28 | TeleWall System | EAL2+ | SecureLogix Corporation | 2000/10 |
| 29 | BorderWare Firewall Server Version 6.5 | EAL4+ | BorderWare Technologies | 2002/01 |
| 30 | Cisco Secure PIX Firewall Software Version 5.2(3) Hardware Models 515, 520 & 525 | EAL4 | Cisco Systems | 2001/02 |
| 31 | Check Point VPN-1/FireWall-1? NG | EAL4 | Check Point Software Technologies Ltd. | 2002/06 |
| 32 | CyberGuard Firewall for UnixWare/Premium Appliance Firewall 4.3 | EAL4+ | CyberGuard Corporation | 2000/12 |
| 33 | Safegate Version 2.0.2 | EAL3 | Fujitsu | 2000/01 |

| 번호 | 제품 | 보증등급 | 공급자 | 인증시점 |
|---|---|---|---|---|
| 34 | SGI IRIX/CMW Version 6.5.13 | EAL3 | Silicon Graphics, Inc. | 2002/04 |
| 35 | SGI Trusted IRIX/CMW Version 6.5.13 | EAL3 | Silicon Graphics, Inc. | 2002/05 |
| 36 | B1/EST-X Version 2.0.1 with AIX, Version 4.3.1 | EAL4 | Bull S.A and IBM Informationssysteme Deutshland Gm | 1999/03 |
| 37 | Sun Solaris(TM) 8 Operating Environment | EAL4 | Sun Microsystems, Inc. | 2000/11 |
| 38 | Cardreader G80-1501 HAD index/10 | EAL1 | Cherry GmbH | 1998/03 |
| 39 | Gemplus 64k Java Card | EAL5+ | Gemplus | 2002/02 |
| 40 | Philips Smart Card Controller | EAL3 | Philips Semiconductors | 1999/11 |
| 41 | UniCert Timestamp Server | EAL3 | Baltimore Technologies Pty Limited | 2002/05 |
| 42 | Bioscrypt Enterprise for NT Logon, Version 2.1.3 | EAL2 | Bioscrypt?Inc. | 2001/06 |
| 43 | IBM Cryptographic Security Chip | EAL3 | Atmel Corporation | 2001/10 |
| 44 | SeNTry 2020 | EAL1 | MIS - Corporate Defence Solutions Ltd. | 1998/07 |
| 45 | Diversinet Passport Certificate Server?Version 4.1.1 | EAL2+ | Diversinet | 2002/05 |
| 46 | 2in1 PC TM Version 1.21 | EAL2 | Voltaire Advanced Data Security | 1999/06 |
| 47 | Entrust TrueDelete Version 4.0 | EAL1+ | Entrust Technologies | 1999/03 |
| 48 | Verisign Processing Center Version 2.5 | EAL4 | VeriSign, Inc. | 2000/01 |
| 49 | Sharp Data Security Kit Version 2.33 | EAL2 | Sharp Electronics Corporation | 2001/04 |
| 50 | SurfinGate Corporate Version 5.6 | EAL3 | Finjan Software, Inc. | 2000/01 |
| 51 | Imagio Neo 350/450 Series | EAL3 | Ricoh Company, Ltd. | 2002/06 |
| 52 | TrustyCabinet UX V1 | EAL3 | Ricoh Company, Ltd. | 2001/01 |

evaluation) 클래스의 보증요구사항들이 아닌 타 보증요구사항들을 적용하는 데 대한 방법론은 정의하고 있지 않다.

ALC_FLR - Flaw Remediation version 1.1 문서는 해석문서인 CCIMB-INTERP-062와 CCIMB-INTERP-092를 포함하여 ALC_FLR 패밀리(Flaw Remediation)의 CC 보증 요구사항을 적용하기 위한 방법론을 제공함으로써 CEM을 보완하고 있다. 이 보완문서는 CCIMB-INTERP-094을 대신한다. 이 패밀리의 보증 컴포넌트들은 CC Part 3의 EAL 어디에도 포함되지 않는데, 이것들은 어떠한 PP와 ST에도 포함될 수 있다. CEM이 추후 갱신된다면 이 문서의 내용은 CEM의 새 버전에는 포함될 예정으로 있다.

그 다음 문서로 2002년 5월에 초안이 발표된 Draft V0.6 Supplement: ASE - Security Target Evaluation Common Criteria and Methodology for Public Review가 있다. 이 문서는 2002년 8월을 목표로 코멘트를 받고 있다[9]. 2002년 5월에 캐나다 오타와에서 열린 CC 관련 학술 회의인 ICCC 2002에서 주제발표를 한 전문가의 얘기로는 CC 프로젝트에서 30~40%의 질문사항이 PP와 ST 관련된 것이라고 하니, ASE 관련 내용 수정은 어쩌면 당연한 일이다. 본 문서는 개정된 ASE 클래스(ST)를 위한 평가기준과 방법론을 제공함으로써 CC와 CEM을 보완하게 된다. 이 문서의 내용은 CC와 CEM이 개정되면 새로운 버전에는 포함될 예정이다.

그 다음 문서로 2002년 7월에 초안이 발표된 Draft V0.68 Supplement: Vulnerability Analysis and Penetration Testing이 있다[10]. 이 문서는 2002년 10월을 목표로 코멘트를 받고 있다. 이 보완 문서는 취약성 분석(AVA_VLA) 패밀리 및 이와 관련한 개념들을 위한 평가기준과 방법론을 대체하게 된다. 이 보완 문서는 취약성 분석에 대한 접근법의 변경의 결과로 수정이 요구되는 아래의 내용물

<표 6> CC 홈페이지에 있는 평가중인 제품 리스트

| 번호 | 제품 | 보증등급 | 공급자 |
|---|---|---|---|
| 1 | Oracle 8i Label Security | EAL4 | Oracle Corporation UK Limited |
| 2 | Symantec Gateway Security V1.0 Enterprise Firewall 7.0 | EAL4 | Symantec Corporation |
| 3 | Dual Concept Fault Tolerance PC Server | EAL2 | Kyokuto Boeki Kaisha Ltd. |
| 4 | Destroy and Destroy Lite | EAL2+ | The Australian Software Company Pty Limited |
| 5 | Cisco IPSEC Crypto System - Versions: Cisco 1700, 2600, 3600, 7100, 7200 routers | EAL4 | Cisco Systems Inc. |
| 6 | Nortel Networks Alteon Switched Firewall | EAL4 | Nortel Networks |
| 7 | StoneGate Firewall and VPN | EAL4+ | Stonesoft |
| 8 | 3Com-Embedded Firewall | EAL2+ | 3Com Business Connectivity Company |
| 9 | Sidewinder Security Server Version 6.0 | EAL4+ | Secure Computing Corporation |
| 10 | SA-400 | EAL2 | Marconi |
| 11 | Sidewinder Firewall & VPN 5.2 | EAL4+ | Secure Computing Corporation |
| 12 | Symantec VelociRaptor Version 1.5 | EAL4 | Symantec Corporation |
| 13 | Cisco Secure PIX Firewall Software Version 6.2 | EAL4 | Cisco Systems |
| 14 | Luna?CA3 Token, Version 3.97 | EAL4+ | Chrysalis - ITS |
| 15 | SurfinShield Corporate Version 5.51 | EAL3 | Finjan Software, Inc. |
| 16 | Protectserver orange c(Host Security Module) Hardware Revision: G | EAL4+ | eracom Technologies Australia Pty Ltd. |
| 17 | Rainbow Technologies iKey - Version: iKey 2000 and iKey 2032 | EAL2 | Rainbow Technologies |
| 18 | Iridian Technologies Private ID, KnoWho Server and Panasonic Authenticam | EAL2 | Iridian Technologies, Inc. |
| 19 | Protectdrive - Version: 5.20 for Windows 98SE, NT 4.0, 2000 and XP | EAL2 | Eracom Technologies Australia Pty Ltd. |
| 20 | Symantec Enterprise Firewall v7.0 for Solaris and W2K | EAL4 | Symantec Corporation |
| 21 | Nokia IPSO Version 3.5 | EAL4 | Nokia Internet Communications |
| 22 | ActivCard Secure Remote Access(SRA) suite of software Version 3.5.0 | EAL2 | ActivCard Canberra Branch Office |
| 23 | DataCryptor 2000 Application Software 3.4, operating on SGSS version 3.1 and DataCryptor 2000 baseboard hardware revision 4a | EAL4 | Thales e-Security(Asia) Limited |
| 24 | Baltimore Technologies Select Access - Version 3.5 | EAL2 | Baltimore Technologies Pty, Ltd. |
| 25 | Owl Computing Data Diode Version 1.0 | EAL2 | Owl Computing Technologies, Inc. |
| 26 | Borderware Mail Gateway 1.3 | EAL4 | Borderware Technologies Inc. |

들을 대체하는 문서이다:

1) 취약성분석 기준(CC v2.1 Clause 14.4);
2) 취약성분석 방법론(CEM v1.0 subclauses 6.9.2, 7.10.3, 8.10.3);
3) 샘플링 전략(CEM Part 2 v1.0 Annex B.2).

이번의 개정으로 비밀채널, SOF(Strength of security Function) 및 오용분석 패밀리에 미치는 효과에 대해서는 현재까지 CCIMB에 의해 완전히 평가되지는 않고 있다. 그래서, 이와 관련한 AVA (vulnerability assessment) 클래스의 하부 패밀리들인 AVA_CCA, AVA_SOF 및 AVA_MSU를 개정하지 못하고 있다. 변경된 접근법을 위한 방법론은 Flaw Remediation 보완 문서(ALC_FLR, version

1.1)에서 소개된 것과 유사한 형식을 취하고는 있지만, CEM Part 2 v1.0에서와 같은 평가 보증레벨에 관련지어서는 설명되지 않고 있다.

# IV. 연구개발체계에 CC 적용

## 1. CC 관련 이슈들

2002년 5월에 캐나다 오타와에서 열린 제 3차 ICCC 회의를 통하여 알게 된 CC 관련 이슈들에 대해 정리하였다[11].

이슈 1) CC 적용과 관련하여 상용 제품이 아닌 시제품(prototype) 개발에도 CC를 적용하는지?

CCIMB의 의장 및 ICCC Track V의 의장을 맡고 있던 Marray Donaldson의 얘기로는 시제품임을 선언하고, 보증 평가를 받으면 된다고 한다. 예를 들면, 시제품의 경우에는 유지보수가 없다는 특징하에 평가를 받으면 된다는 것이다.

이슈 2) 보증 등급은 CC에서 적용하는데 기능 등급은 전혀 고려치 않고 있는 것 같은데, CC에 기능등급이 있는지?

Marray Donaldson의 얘기로는 CC에는 기능 등급은 없다고 한다. 왜냐하면, 보안 제품의 종류 및 기능이 너무나 다양하므로 기능 등급을 정하지 않았으며, 사실 기능 등급을 정할 필요도 없다는 것이다. 왜냐하면, CC 등급이란 평가 대상 IT 제품에 대한 보안 보증등급이기 때문이다.

이슈 3) 그렇다면, 왜 EAL이 TCSEC이나 ITSEC의 등급에 맞추어 테이블 형태로 홈페이지나 관련 자료에 기술되어 있는가?

그 이유는 CC를 처음 소개할 때, 이미 많은 사람들이 기존의 평가 기준인 TCSEC이나 ITSEC에 익숙하였기 때문에 CC를 효과적으로 소개하기 위한 수단으로 그렇게 표현하였던 것이지 TCSEC의 등급 혹은 ITSEC의 등급과 CC의 EAL과의 1:1 상호관계는 없다.

이슈 4) 한 시스템에서 EAL 등급 적용을 어떤 단위로 하고, 전체 시스템에 대해서 EAL 등급을 적용할 수 있는지?

Marray Donaldson 및 ICCC 튜토리얼 강사였던 Michael A. McEvilley의 얘기로는 여러 개의 IT 제품으로 컴포지션(composition)된 시스템 전체에 대한 EAL 등급을 받는 것보다는 IT 제품 각각에 대하여 EAL 등급을 받는 것이 합리적이라는 것이다. CC는 여러 개의 IT 제품으로 구성된 시스템에서의 제품간의 인터페이스, 즉 컴포지션에 대한 평가는 직접적으로 언급하고 있지 않다고 한다.

ICCC'2002에서는 다음과 같은 세션에서 이 문제를 다루고 있었다.

- 14일 Technical Session: "Practical application of the CC to support Systems Security Engineering"
- 14일 Evaluation/Certifier Workshop: "ASE_ENV and Composition"
- 14일 Evaluation/Certifier Workshop: "TOE Requirements to Support Composition"

위의 세션 가운데 "Evaluation/Certifier Workshop"에서 현재의 CC 버전에는 직접적으로 IT 제품들의 컴포지션 평가를 다루고 있지 않으므로, 이에 대한 대안책으로 현재의 CC를 어떻게 활용하여 컴포지션을 평가할 수 있는가를 제안한 발표가 있었는데 그 내용은 다음과 같다.

컴포지션이란 "두 개 또는 그 이상의 IT 제품들의 통합"을 뜻하는 것으로 각각 평가를 받은 두 개의 독립적인 제품의 컴포지션이나 평가를 받은 제품과 평가를 받지 않은 제품의 컴포지션을 생각할 수 있다. 제품간의 인터페이스를 그 제품이 작동되기 위해 필요한 IT 환경요구사항으로 고려함으로써 CC 평가 체계를 사용할 것을 제안한다. 예를 들어서 데이터베이스 제품과 OS 제품의 컴포지션이라

면, 데이터베이스 제품과 OS 제품과의 통신을 위한 TSFI(TOE Security Function Interface)를 평가 대상으로 하여, 개발자의 경우는 ST, AGD_ADM, ADV_HLD에 해당하는 평가제출물을 작성하고, 평가자는 환경설명, 보안 요구사항 및 SFR(Security Functional Requirement), TSF policy를 분석하고 시스템 형상의 완전성을 시험한다.

이슈 5) EAL 등급 결정은 어떻게 하는지?

튜토리얼 세션 2: “Common Criteria: not just for evaluation anymore”의 강사의 얘기로는 등급의 결정은 IT 제품 종류에 따라 구분되는 것이 아니고, 제품 개발에 관한 예산과 직접적인 관련이 있다고 보는 것이 맞다고 한다.

13일 “Reception and Awards” 세션에서 각 인증국가에서 올해 인증 받은 IT 제품에 대한 인증서 수여식이 있었다. 이 때 인증서 받은 대부분의 제품, 특히 스마트 카드에 관한 제품은 EAL 4 혹은 EAL 5 이었다.

## 2. 연구개발체계에 CC 적용 시 보증 증거물들

연구개발을 추진하는 연구기관이나 업체의 입장에서는 CC 적용에 따른 증거물(evidence)로 어떤 문서를 어느 수준으로 만들어내야 하는가 하는 것은 중요하고도 실질적인 문제이다. <표 7>에서는 CC/EAL 4를 개발체계에 도입함에 따라 개발의 확실성을 보증하기 위해 요구되는 개발체계상의 기술문서들을 ETRI에서 추진했던 사업의 개발체계를 참고로 하여 살펴보았다[12].

EAL 4를 위한 증거물들은 서술식으로 작성하면 되므로 증거물들 작성시 UML(Unified Model Language) 등의 준정형의 언어를 꼭 사용할 필요는 없으므로 기존의 개발체계의 문서작성법과 별반 차이가 없으나, 개발의 확실성을 보증하기 위해 세부 개발단계간 일치성을 검증하기 위한 분석 자료들 및 보안에 문제가 있는지를 분석하는 자료들이 많이 요구되는 것이 특징이다.

<표 7> CC 보증 클래스와 연구개발체계상의 결과물과의 관계

| 보증클래스 | 보증컴포넌트 | 개발체계상의 결과물 |
|---|---|---|
| ASE | | ST(보안목표명세서) |
| ACM | ACM_AUT.1<br>ACM_CAP.4<br>ACM_SCP.2 | 형상관리지침서<br>형상관리지침서<br>형상관리지침서 |
| ADO | ADO_DEL.2<br>ADO_IGS.1 | 기술이전절차서<br>사용자 매뉴얼 |
| ADV | ADV_FSP.2<br>ADV_HLD.2<br>ADV_IMP.1<br>ADV_LLD.1<br>ADV_RCR.1<br>ADV_SPM.1 | 개발기능규격서<br>시스템설계서/서브시스템설계서/기능설계서<br>SPF(Source Program File) 및 PBA 설명서<br>블록설계서/유닛설계서<br>검증명세서<br>보안정책모델서 |
| AGD | AGD_ADM.1<br>AGD_USR.1 | 사용자 매뉴얼<br>사용자 매뉴얼 |
| ALC | ALC_DVS.1<br>ALC_LCD.1<br>ALC_TAT.1 | 문서관리지침서/보안지침서<br>순기관리지침서/진도관리지침서<br>개발 툴 선정 보고서 |
| ATE | ATE_COV.2<br>ATE_DPT.1<br>ATE_FUN.1<br>ATE_IND.2 | 기능규격 일치성 분석서<br>시스템설계 일치성 분석서<br>시험절차서(계획,예상결과 포함) 및 시험결과서<br>시제품/시험환경구축계획서 |
| AVA | AVA_MSU.2<br>AVA_SOF.1<br>AVA_VLA.2 | 사용자매뉴얼 오용 분석서<br>보안성 분석서(보안기능 강도)<br>보안성 분석서(취약성) |

상기 보증 클래스와 보증 컴포넌트 이름은 CC Part 3 version 2.1에 있는 약자를 그대로 사용한 것이며, 결과물들의 이름은 연구개발체계상의 공식 기술문서 명으로 가능한 표현한 것이다.

# V. 맺음말

본 고에서는 먼저, 기존 정보보호시스템 평가기준인 TCSEC과 ITSEC에 대해 살펴 본 후, 최근에 국제간에 상호 인증을 받을 수 있는 정보보호시스템 공통평가기준(CC)에 대해 CC 출현 배경, CC 구성 내용, PP와 ST 개발동향, CC의 최근 표준화동향 등으로 나누어 살펴보았다. 그리고, 연구개발을 추진하는 개발자 입장에서 연구개발체계에 CC를 어떻게 적용할 것인가에 대한 방안을 살펴보았다. 이를 위해 먼저, CC 관련 주요 이슈들에 대해 ICCC2002를 통해 알게 된 내용을 위주로 살펴보고, 연구개발

체계에 CC 도입 시 개발자들이 증거물로 제시해야 할 결과물에 대해 제시하였다.

이제 CC의 도입은 거를 수 없는 대세로 자리 잡고 있으며, 국내에서도 CC를 도입하기 위해 인증기관, 평가기관 차원뿐만 아니라 개발자 입장에서도 만반의 준비를 하는 것이 필요하다고 생각된다. 따라서, 본 고는 CC를 고려하여 정보보호시스템을 개발하고자 하는 연구기관 및 업체에서 개발전략을 수립할 때 참고사항으로 사용될 수 있을 것으로 생각된다.

## 참 고 문 헌

[1] ISO/IEC International Standard(IS) 15408, Parts 1 thru 3, Aug. 1999.

[2] 시스템 보안 평가 규격 및 평가 도구 연구, 위탁연구보고서, 한국전자통신연구원, 2001.

[3] ISO/IEC PDTR 15446 Information technology techniques - Guide for the production of protection profiles and security targets, Apr. 2000.

[4] http://www.commoncriteria.org

[5] 제7회 정보보호심포지엄 SIS 2002, 2002. 7. 9~10., pp. 314 - 315.

[6] CEM document, Part 1, version 0.6, Jan. 1997.

[7] CEM document, Part 2, version 1.0, Aug. 1999.

[8] ALC_FLR - Flaw Remediation, version 1.1, Feb. 2002.

[9] Draft V0.6 Supplement: ASE - Security Target Evaluation Common Criteria and Methodology for Public Review, Draft, May 2002.

[10] Draft V0.68 Supplement: Vulnerability Analysis and Penetration Testing, Draft, July 2002.

[11] ICCC 2002 출장결과보고서, 한국전자통신연구원, 2002.

[12] ETRI 정보보호연구본부, "연구개발체계," version 1.0, June 2002.

[13] 정보보호시스템 평가 인증 가이드, 한국정보보호센터, 2000.